

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2000-503198

(P2000-503198A)

(43) 公表日 平成12年3月14日 (2000.3.14)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
H 0 4 L 12/56		H 0 4 L 11/20	1 0 2 Z
12/28		H 0 4 M 3/00	B
12/46		11/00	3 0 3
12/66		H 0 4 L 11/20	B
29/08		13/00	3 0 7 Z
審査請求 有 予備審査請求 未請求(全 53 頁) 最終頁に続く			

(21) 出願番号 特願平11-507419
 (86) (22) 出願日 平成10年7月2日(1998.7.2)
 (85) 翻訳文提出日 平成11年3月3日(1999.3.3)
 (86) 国際出願番号 P C T / U S 9 8 / 1 3 8 5 8
 (87) 国際公開番号 W O 9 9 / 0 1 9 6 9
 (87) 国際公開日 平成11年1月14日(1999.1.14)
 (31) 優先権主張番号 0 8 / 8 8 7 , 3 1 3
 (32) 優先日 平成9年7月3日(1997.7.3)
 (33) 優先権主張国 米国 (U S)

(71) 出願人 スリーコム コーポレイション
 アメリカ合衆国 イリノイ ローリング
 メドウズ ゴルフ ロード 3800
 (72) 発明者 ユイ イーチュン
 アメリカ合衆国 イリノイ パファロー
 グローヴ チェスナット コート ウェス
 ト 36
 (72) 発明者 ベネット エス カードウェル
 アメリカ合衆国 イリノイ エヴァンスト
 ン リース アヴェニュー 2749
 (74) 代理人 弁理士 矢野 敏雄 (外2名)

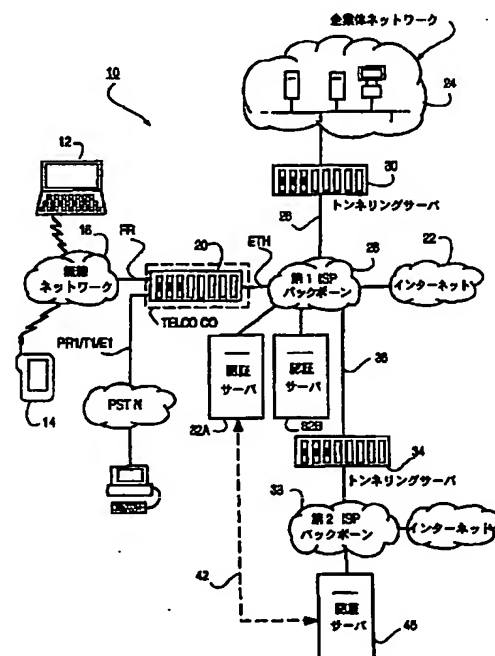
最終頁に続く

(54) 【発明の名称】 インターネットへのダイレクトワイヤレスアクセスを含む、ネットワークアクセス方法

(57) 【要約】

デジタルデータ源をコンピュータネットワークに接続する方法。デジタルデータ源はワイヤレス伝送オフアクセス伝送媒体を介してワイヤレスサービスキャリアにデータを伝送し、ワイヤレスサービスキャリアにより該データが多重化され高速デジタル電話回線に送出される。この方法は以下のステップ：デジタルデータをネットワークアクセスサーバ等の通信シャシにおいて受け取り、該デジタルデータから、少なくとも (a) デジタルデータ源の呼び出した電話番号又は (b) デジタルデータ源に関連した電話番号を含むネットワークアクセス認証データを抽出し；認証データを、該コンピュータネットワーク用のネットワーク認証サーバに接続されたローカル又はワイドエリアコンピュータネットワークを介して伝送し；ネットワーク認証サーバにおいて、伝送された認証データに基づいて該遠隔ユーザに対してコンピュータネットワークへのアクセスが許可されているかどうかを判断し；認証サーバは認証アクセスサーバに対して判断ステップの結果を通知し；判断ステップの結果が肯定であればデータ源に対してコンピュータネッ

FIG. 1



BEST AVAILABLE COPY

【特許請求の範囲】

1. デジタルデータ源をコンピュータネットワークに接続する方法において、前記デジタルデータ源はワイヤレス伝送媒体を介してワイヤレスサービスキャリアと通信を行い、前記ワイヤレスサービスキャリアは前記デジタルデータを多重化し高速デジタル電話回線に送出するよう構成されており、前記方法が

前記デジタルデータを、電話回線インタフェース及びネットワークインタフェースを有する通信装置において受け取り、

前記通信装置は前記デジタルデータからアクセス認証データを抽出し、前記認証データは少なくとも (a) 前記デジタルデータ源により呼び出された電話番号、又は (b) 前記デジタルデータ源に関連付けられた電話番号のいずれかを有し、

前記通信装置は前記認証データを、前記ネットワークアクセスサーバに接続されたローカルエリア又はワイドエリアコンピュータネットワークを介して、前記コンピュータネットワーク用のネットワーク認証サーバに伝送し、

前記ネットワーク認証サーバ内において、前記伝送された認証データに基づいて、前記遠隔ユーザが前記コンピュータネットワークに対してアクセス許可されているかどうかを判断し、

前記認証サーバは、前記通信装置に対して、前記判断ステップの結果を通知し、判断結果が肯定的であれば前記コンピュータネットワークに対するアクセスを前記デジタルデータ源に許可する、という各ステップを有していることを特徴とする方法。

2. 前記認証サーバにおいて、前記通信装置に結合されており、前記デジタルデータ源に対して前記コンピュータネットワークへのアクセスを与えるためのトンネリングサーバを識別し、

前記デジタルデータ源からのデジタルデータを前記トンネリングサーバにルーティングすることにより、前記アクセスを前記コンピュータネットワークに与えるステップを更に有した、請求項1記載の方法。

3. 前記認証サーバにおいて、前記デジタルデータ源のための、すなわち前

記デジタルデータを前記ネットワークアクセスサーバと前記トンネリングサーバとの間でトンネリングするためのトンネリングプロトコルを決定し、

前記デジタルデータ源からのデジタルデータを前記トンネリングプロトコルに従って前記トンネリングサーバにルーティングするステップを更に有した、請求項2記載の方法。

4. 前記トンネリングプロトコルが、PPTP及びTELNETを含むプロトコル群から選択される、請求項2記載の方法。

5. 前記コンピュータネットワークがインターネットを含む、請求項1記載の方法。

6. 前記コンピュータネットワークが企業ローカルエリア又はワイドエリアネットワークを含む、請求項1記載の方法。

7. 前記通信装置が公衆交換電話網にアクセスを供給し、前記通信装置は、前記判断ステップにおいて否定的反応が得られた場合に、前記公衆交換電話網を介して前記デジタルデータを目的地にルーティングするよう試みるよう構成された、請求項1記載の方法。

8. (1) 前記トンネリングサーバ又は(2) 前記認証サーバと前記デジタルデータ源との間でパスワード認証ルーチンを実行し、前記デジタルデータ源と前記コンピュータネットワーク間で第2レベルの認証を行うよう構成された、請求項2記載の方法。

9. 高速電話回線を介してユーザからの電話呼出を受け取るよう構成された通信装置を有したインターネットサービスプロバイダのためのインターネットアクセス方法において、

前記通信装置を、ローカル又はワイドエリアネットワークを介して認証サーバに接続し、

前記ユーザからの入力呼出から、少なくとも(a) 前記ユーザにより呼び出された電話番号又は(b) 前記ユーザに関連付けられた電話番号のいずれかを有するネットワークアクセス認証データを抽出し、

前記ネットワーク認証データを前記認証サーバにルーティングし、前記ネットワークアクセス認証データに基づいて前記ユーザの認証を行い、

前記ユーザに対してネットワークアクセスを与えるためのトンネリングサーバを識別し、前記ネットワークアクセスサーバに前記トンネリングサーバを通知し、

前記ネットワークアクセスサーバからのデジタルデータを前記トンネリングサーバにトンネリングし、

前記トンネリングサーバにより前記デジタルデータをインターネットに送る、という各ステップを有した方法。

10. 前記トンネリングステップにおいて前記ユーザのためのトンネリングプロトコルを識別するステップを更に有した、請求項9記載の方法。

11. デジタルデータを発生するコンピュータをインターネットに接続する方法において、前記デジタルデータは高速デジタル電話回線を介してインターネットサービスプロバイダに伝送されるよう構成されており、

前記デジタルデータを、前記インターネットサービスプロバイダの通信装置において受け取り、

前記デジタルデータから、少なくとも(a)前記デジタルデータ源により呼び出された電話番号又は(b)前記コンピュータに関連付けられた電話番号のいずれか、を有するインターネットアクセス認証デー

タを抽出し、

前記認証データをネットワーク認証サーバに伝送し、

前記ネットワーク認証サーバ内で、前記伝送された認証データに基づいて、前記遠隔ユーザが前記ネットワークアクセスサーバを介してインターネットにアクセスすることが許可されているかどうかを判断し、

前記認証サーバは前記ネットワークアクセスサーバに、前記判断ステップの結果を通知し、前記判断ステップにおいて肯定的反応が得られた場合は前記コンピュータに対してインターネットへのアクセスを許可する、という各ステップを有した方法。

12. コンピュータがインターネットにアクセスするために使用するトンネリングサーバを、前記認証サーバ内で識別し、

前記コンピュータからのデジタルデータを前記トンネリングサーバにルーティングし、インターネットへの前記アクセスを供給するという各ステップをさらに有した、請求項11記載の方法。

13. 前記認証サーバにおいて、前記ネットワークアクセスサーバと前記トンネリングサーバ間でデジタルデータをトンネリングするために使用するトンネリングプロトコルを決定し、

前記コンピュータからのデジタルデータを、前記トンネリングプロトコルに従って前記トンネリングサーバにルーティングするという各ステップを更に有した、請求項12記載の方法。

14. 前記トンネリングプロトコルが、PPTP及びTELNETを含むプロトコル群から選択される、請求項13記載の方法。

15. 前記通信装置が公衆交換電話網にアクセスを供給し、前記通信装置は、前記判断ステップにおいて否定的反応が得られた場合には前記公衆交換電話網を介して前記デジタルデータを目的地にルーティングするよう試みるよう構成されている、請求項11記載の方法。

16. (1) 前記トンネリングサーバ又は(2) 前記認証サーバと前記コンピュータとの間でパスワード認証ルーチンを実行し、前記デジタルデータ源と前記コンピュータネットワークとの間で第2レベルの認証を実行するよう構成された、請求項12記載の方法。

17. ワイヤレスインターネットユーザのためのインターネットサービスプロバイダシステムにおいて、

ネットワークアクセスサーバと、

インターネットアクセス認証サーバとを有し、

前記ネットワークアクセスサーバは高速デジタル電話回線インタフェースとインターネットゲートウェイを有し、該インタフェースは前記ワイヤレスインターネットユーザからの呼出を受け取り、該ゲートウェイは、前記ワイヤレスイン

ターネットユーザに関連付けられたデジタルデータをインターネットに送出し

、
前記インターネットアクセス認証サーバは通信媒体を介して前記ネットワークアクセスサーバに接続され、前記インターネットアクセス認証データに応答するよう構成され、該認証データは、前記ワイヤレスインターネットユーザに関連付けられた前記デジタルデータから抽出され、また前記デジタルデータは前記ネットワークアクセスサーバにより受け取られ前記認証サーバに伝送されたものであり、

前記認証サーバはさらにメモリを備え、それによって、前記インターネットアクセス認証データに基づいて、前記ワイヤレスインターネットユーザがインターネットに対してアクセス許可されているかどうかを判断し、前記インターネットサーバは前記ネットワークアクセスサーバに認証反応を送信し、

前記ネットワークアクセスサーバは前記認証サーバからの前記認証反応に応答し、前記ワイヤレスインターネットユーザに対してインターネットへのアクセスを許可するが、又は該ワイヤレスインターネットユーザからの呼出に関してその他の動作を行うよう構成された、インターネットサービスプロバイダシステム。

18. 前記ネットワークアクセスサーバと通信媒体を介して結合された第2インターネット認証サーバを有し、

前記第2インターネット認証サーバは前記ネットワークアクセスサーバからの認証データに反応するよう

構成され、また第2のインターネットサービスプロバイダにより管理され、

更に前記第2インターネット認証サーバは前記ワイヤレスインターネットユーザに対して、前記ネットワークアクセスサーバ又は前記インターネットアクセス認証サーバの何れかに対する認証反応を与えるよう構成されている、請求項17記載のインターネットサービスプロバイダシステム。

【発明の詳細な説明】

インターネットへのダイレクトワイヤレスアクセスを

含む、ネットワークアクセス方法

発明の背景**A. 発明の分野**

この発明はデータ通信の分野に関し、特にワイヤレスユーザにより発生されたデジタルデータ（携帯電話モデムを有したコンピュータ等）を、社内LANやインターネットなどのコンピュータネットワークに接続する方法に関する。

B. 関連技術の説明

公衆交換電話網からダイヤルしている遠隔ユーザに対してローカル又は広域ネットワークへのアクセスを可能にするネットワークアクセスサーバが公知である。このような装置は3COM社（以前はU.S. Robotics Access Corp.）、すなわち本願の譲受人から入手可能である。3COM社の総合制御ネットワーク企業体ハブ（Total Control Network Enterprise Hub）が代表的なネットワークアクセスサーバである。このサーバは、Baum他の米国特許第5577105号：「データ通信用の電話呼出交換及びルーティング方法」に、また、Walsh他の米国特許第5528595号：「モデム

入出力信号処理方法」に記載されている。Walsh他及びBaum他の特許は何れも本願明細書に引用する。

Walsh等及びBaum等の特許に記載されたネットワークアクセスサーバは、多重デジタル電話回線へのインタフェース、遠隔ユーザからのデータを信号変換するための複数のモデム、及びモデムからの復調データをローカル又はワイドネットワークへ伝送するためのネットワークインタフェースを有する。時分割多重バスを有する高速ミッドプレーンバス構造は、電話回線のチャネルとモデム間の信号路として機能する。この高速ミッドプレーンは、モデムとネットワークインタフェースを結合する並列バスも含む。

単一のシャシにおけるこのネットワーク・アクセス・サーバ・アーキテクチャは様々なアプリケーション、特に企業ネットワークアクセスの分野において非常

に人気が高い。このネットワーク・アクセス・サーバ・アーキテクチャはまた、陸上インターネットユーザに対するインターネットサービスプロバイダにも人気が高い。1つのネットワークアクセスサーバにより、インターネットサービスプロバイダは多数の同時インターネットアクセス呼出に対処し、複数の遠隔ユーザとインターネット上のホストコンピュータ間において全二重通信を供給することができる。

ワイヤレスユーザに対してインターネットアクセスを可能にする技術が出現しつつある。ワイヤレスサ-

ビスには2つの競合する標準、すなわちCDMA（符号分割多重アクセス。標準文書IS-130及びIS-135に記載。参照として本願明細書に引用。）と、TDMA（時分割多重アクセス。標準文書IS-99に記載。同じく参照として本願明細書に引用。）がある。これらの標準は、音声とデータ両方のための機能の豊富なデジタル無線通信の形式を規定している。この2つの標準は、複数のユーザからのデジタルデータがどのように無線インターフェース上で多重化されるかという点で異なる。

いずれの無線技術においても、ワイヤレスユーザはデータを移動交換センタへ送信する。移動交換センタは公衆交換電話網に対する接続を可能にし、特定の多重・制御機能を果たし、移動ユーザに対して交換機能を提供する。それによって、複数のワイヤレスユーザからの多重化デジタルデータを高速通信フォーマット（フレームリレー等）を介して、公衆交換電話網内の通信要素に送ることが可能となる。

本願の発明は、特にワイヤレスユーザに適した、ネットワークアクセス方法及び装置を提供する。本願発明のネットワーク・アクセス方法によれば、ネットワークアクセスサーバと、1つ又は複数の認証サーバが協働して、インターネット及び企業ネットワーク認証及びアクセスを供給することが可能となる。ネットワークアクセスサーバは、TDMA又はCDMA移動電

話に接続された端末装置と、公衆交換電話網（PSTN）及びインターネットに

接続された端末装置とが協働するために必要な機能を提供する。さらに、本発明によれば、複数のインターネットサービスプロバイダに加入している複数の遠隔ユーザのためのインターネットアクセス方法が提供され、インターネットサービスプロバイダは様々なインターネットユーザに対してより柔軟なサービスを提供することが可能となる。

発明の要旨

デジタルデータの発生源をコンピュータネットワークに接続する方法が提供される。このデジタルデータ源はデジタルデータを発生するとともに、ワイヤレス送信媒体を介してワイヤレスサービスキャリアとの通信を行う。ワイヤレスサービスキャリアはデジタルデータを高速デジタル電話回線上に多重化し、ネットワークアクセスを提供する通信シャシ又はサーバに送信する。本発明の方法は通信シャシ上でデジタルデータを受け取り、デジタルデータから、少なくとも、(a) デジタルデータ源により呼び出された電話番号、又は (b) デジタルデータ源と関連付けられた電話番号、のうち1つを含むネットワークアクセス認証データを取り出す。通信シャシは、ネットワークアクセスサーバに接続されたローカルエリア又はワイドエリアコンピュータネットワークを介し

て、認証データを、コンピュータネットワーク用のネットワーク・認証・サーバに送信する。ネットワーク認証サーバは送信された認証・データに基づいて、遠隔ユーザがコンピュータネットワークにアクセスすることが許可されているかどうかを判断する。認証サーバは従って、ネットワークアクセスサーバに判断の結果を知らせる。遠隔ユーザは、判断ステップの結果が肯定であれば、コンピュータネットワークへのアクセスが許可される。

この方法はさらに、ローカルエリア又はワイドエリアネットワークを介して通信シャシにリンクされたトンネリングサーバを認識し、データ源からのデジタルデータをトンネリングサーバにルーティングしてコンピュータネットワークへのアクセスを提供するステップを含むことができる。前記トンネリングサーバはデジタルデータ源に対して、コンピュータネットワークへのアクセスを与えるものである。トンネリングサービスの識別は遠隔ユーザからの認証データに基づ

いて行われ、該データは遠隔ユーザの電話番号やダイヤルされた番号等である。この実施例では、認証サーバにおいて、デジタルデータ源からのデジタルデータを通信装置とトンネリングサーバ間でトンネリングするためのトンネリングプロトコルを決定することもできる。この決定ステップは、例えば、遠隔ユーザ（該ユーザの電話番号等により識別）に関連付けられ

たトンネリングサーバと必要なプロトコルをソフトウェアルックアップテーブルから見つけたすことにより実行可能である。デジタルデータはトンネリングプロトコルに従って、トンネリングサーバを介してルーティングされる。好適な実施例では、PPTP又はTELNETプロトコルが使用される。

アクセス認証の第2段階がオプションとして行われる。これは、遠隔ユーザと認証サーバ又はトンネリングサーバ間で行われるパスワード認証ルーチンから構成される。

本発明の主要な目的は、従って、ワイヤレスユーザ等の遠隔ユーザに対して、インターネットその他のコンピュータネットワークへの直接的アクセスを供給することである。この目的及びその他の目的は以下の詳細な説明から明らかとなる。

図面の簡単な説明

現在のところ好適と考えられる本発明の実施例を図面を参照して説明する。図面において、同一の参照番号は同一の要素を示す。

図1は本発明の実施例におけるワイヤレスユーザ用に好適なネットワークアクセスシステムの一例である。

図2は、図1の通信シャシの好適な一形態の機能ブロック図である。該通信シャシはワイヤレスユーザのみならず、公衆交換電話網を介してダイヤルするユーザをも取り扱うことができる。

図2Aは、アナログモデム呼出に対応していない実施例に適した通信シャシのブロック図である。

図3は、遠隔ユーザと図1のトンネリングサーバ間のトンネルインタフェース

用プロトコルスタックである。

図4は、通信シャシと図1の認証サーバ間の認証及び課金インタフェース用のプロトコルスタックである。

図5は、リモートダイアルユーザと、該ユーザを目的地端末装置に接続するルータとの間の非トンネリングインタフェースのプロトコルスタックである。

図6は本発明の好適な実施例における、呼出受入シナリオにおけるトンネリング用PPTPプロトコルの呼出フローである。

図7は本発明の好適な実施例における、呼出受入シナリオのトンネリング用TELENETプロトコルの呼出フローである。

図8は、認証失敗シナリオにおける呼出フローである。

図9は、トンネリングサーバアクセス拒絶シナリオにおける呼出フローである。

図10は、PPTPプロトコルにおいてログインパスワード認証がネットワークアクセス認証プロシージャの第2段階として実行された場合における、認証失敗シナリオの呼出フローである。

図11は、TELENETにおいてログインパスワード認証がネットワークアクセス認証プロシージャの第2段階として実行された場合における、認証失敗シナリオの呼出フローである。

好適な実施例の詳細な説明

図1には、本発明の実施に好適なネットワークアクセスシステム10が示されている。このシステムは無線装置12、14のユーザにより使用される。無線モデムを備えたラップトップコンピュータ、又は無線パーソナルデータアシスタント(PDA)14等の遠隔装置は、無線モデムを介して、TDMA(時分割多重アクセス)又はCDMA(符号分割多重アクセス)標準に従って、無線デジタル通信ネットワークと通信を行う。

ワイヤレスネットワーク16はモバイルスイッチングセンタ(MSC)(図示しない)を含む。移動交換センタは無線通信ネットワーク16内の要素であり、

ワイヤレスユーザに対して公衆交換電話ネットワークへの接続、制御機能及び交換機能を提供する。図1の実施例では、ワイヤレスユーザからのデータはMSCにより高速デジタルフレームリレー回線FRに乗せられ、ローカル呼び出しエリア内の通信シャシ20に送信される。好適な実施例では、通信シャシ20は3Com社（前身はU. S. Robotics）の総合制御ネットワーク企業体ハブ（Total Control Network Enterprise Hub）等の統合ネットワークアクセスサーバを有する。この場合、該サーバはフレームリレー回線FRとインターフェースし、後述するトンネリング、認証、及びアカウンティング機能を行うよう修正される。

通信シャシ20は、CDMA/TDMAワイヤレスネットワーク16とインターネットサービスプロバイダ（ISP）バックボーンネットワーク26、インターネット22又はその他のローカルエリアネットワークETHとインターネットサービスプロバイダバックボーンネットワーク26間のゲートウェイとして機能する。シャシ20は、CDMA又はTDMA移動電話に接続された端末装置がPSTN及びインターネットネットワークに接続された端末装置と相互に通信を行うために必要な機能を提供する。好適な実施例では、通信シャシ20は電話会社本社（telephone company central office; TELCO CO）内に配置され、インターネットサービスプロバイダ（ISP）により維持される。シャシ20はワイヤレスユーザ12、14からの呼び出しをワイヤレスネットワーク16内のMSCを介して、回線FR上のローカル呼び出しとして受け取る。

無線端末12、14は企業/個人ネットワーク24にアクセスするために、通信シャシ20とトンネリングサーバ30間のLAN又はWAN回線28を介して、トンネリングプロトコルを利用する。トンネリングサーバは企業/プライベートネットワーク24に接続され、かつバックボーンネットワーク26を介して通信シャシ20に接続されている。好適な実施例では、トンネリングは、一般に入手可能であるRFC文書で

あるPPTPRFC（1996年6月）に記載されたポイントツーポイント・トンネリングプロトコル（PPTP）に従う。このRFC文書は参照として本願明

細書に引用する。トンネリングは勿論、その他の登場しつつある同等のプロトコル、例えばL2TPに従うことも可能である。PPTPとL2TPは非PPP非同期プロトコルを支援するよう設計されていないので、非PPP非同期トラフィックを回線28上でトンネリングするためにはTELENETプロトコルを使用する。トンネリングサーバはまた、好適には、前述のトータル・コントロール・エンタープライズ・ネットワーク・ハブないし同等の統合ネットワークアクセスサーバである。

このようなアーキテクチャにおいて、当初のダイアルアップ・サーバ（通信シャシ20）の場所を、中間ネットワークがダイアルアップ・プロトコル接続（PPP）を切断し、トンネリングサーバ30において目標とするネットワーク22又は24にアクセスを与える場所から分離することができる。目標ネットワークとしてのインターネット22を支援することに付け加えて、このアーキテクチャは仮想個人ネットワークへのアクセスを支援することにより、ワイヤレスユーザに対して、該ユーザの企業又はプライベートネットワーク、例えば図1の企業体ネットワーク24に確実にアクセスすることを可能にする。

このアーキテクチャにより更に、前記本社（CO）におけるローカル通信シャシ20を管理しているインターネットサービスプロバイダは、ISPクライアントだけでなく、他のインタフェースサービスプロバイダのクライアントに対してもインタフェースアクセスを提供することが可能となる。これは、インターネットサービスプロバイダのバックボーンネットワーク26に接続された一つ又は複数の認証サーバ32A、32Bを利用することにより達成される。認証サーバ32A、32Bは最初のISPクライアントに対する認証とアクセス許可を実行する。第2のトンネリングサーバ34は専用線36（又はLANないしWAN）を介して又は直接に第2のISPのバックボーンネットワーク38に接続される。この実施例では、認証サーバ32Aは通信シャシ20を運営している第1のISP用のクライアントリストを有しており、後述するような様々な簡単な方法を用いて、通信装置20にダイアルしている遠隔ユーザが、ISPのバックボーン26を介してインターネット22にアクセスすることが許されているかどうかを判

断できる。(当該呼出が第1インターネットサーバプロバイダのクライアントの一人から行われているため)アクセスが認められていれば、当該呼出はネットワーク22を介してインターネットにルーティングされる。そうでなければ、後述するような他のプロシージャが開始される。

本発明は、遠隔ユーザからの呼出には発信者の電話番号とダイアルされた電話番号を示す情報が含まれていることを利用する。この情報は第1段階の認証機構として使用される。認証サーバ32Aがこの第1段階認証を実行し、遠隔ユーザが第1インターネットサーバプロバイダのクライアントでなく(例えば電話番号がクライアント電話番号リストと一致しないため)、第2のインターネットサービスプロバイダのクライアントであると判断された場合、認証サーバ32Aは認証要求を、第2インターネットサービスプロバイダのバックボーン38に接続された第2の認証サーバ40に送り、第1段階認証が行われる。この通信は専用線42(専用通信回線、POTS回線等)を認証サーバ32Aと、第2のインターネットサーバプロバイダにより運営されている認証サーバ40との間に設けることにより円滑化される。

認証の結果が肯定であれば、認証サーバ40は認証サーバ32Aに結果を通知し、ワイヤレスユーザ12はネットワーク26又はトンネリングサーバ34を介してインターネット22に対するアクセスが与えられるか、又は、遠隔ユーザ12と第2認証サーバ40の間でオプションとして第2段階のパスワード式の認証が行われる場合もある。

このような特徴の組み合わせにより、通信シャシ20並びに認証サーバ32Aを運営しているISP又は

その他の組織に対して、それらがクライアントに提供するサービスを大幅に増加する能力が与えられる。また、この組み合わせにより、ISPは他のインターネットサービスプロバイダに対してもインターネットアクセスを提供することが可能となり、その過程でそのようなサービスに対する収益がおそらく生ずる。ワイヤレスユーザから見れば、ワイヤレスネットワーク16を介しての通信装置20

へのローカル呼出により、インターネット又は企業ネットワークへアクセスできる。

本発明の好適な実施例では、通信シャシ20は統合汎用コンピュータプラットフォームを備えた前述の総合制御ネットワーク企業体ハブ等の強力な通信プラットフォーム、すなわち3COM社から入手可能なEdgeServerTMである。この製品を利用することにより、通信シャシは、マイクロソフト社のウィンドウズNT等の市販の独立型オペレーティングシステムや、その他の遠隔アクセスソフトウェア製品、例えばRADIUS (Remote Authentication Dial In User Service) を動作させることが可能となる。上述のインターネットアクセス方法では、好適には、課金及び認証機能はRADIUSプロトコル、又はその他の市販又は公知の課金ソフトウェアプログラムを利用して使用される。RADIUSプロトコルは公知のプロトコルであり、本願明細書に参照として引用するRFC2058、199

7年1月、に記載されている。

本発明の好適な実施例では、2段階の認証により、インターネット22又は企業/プライベートネットワーク24に対するアクセスが、ネットワーク26を介してのアクセスが認められているワイヤレスユーザに対してのみ与えられる。認証の第1段階は、遠隔ユーザ12、14によりダイヤルされた番号と、ワイヤレスユーザ12、14の発信者の番号（すなわちコンピュータ12又はPDA14に関連付けられたユーザの電話番号）に基づいて行われる。認証の第2段階は、テストユーザ名及びパスワード認証プロトコル（PPP及びTELLNETトンネリング用）に基づいて行われるか、又はチャレンジ/レスポンスプロトコル（PPPトンネリング専用）に基づいて行われる。これらの認証プロシージャの詳細は以下に説明する。

図1において、通信装置20はまた好適には、通信装置内のインターネットインタフェースから直接の、すなわちトンネリングを介さないインターネット22へのアクセスも支援する。この機能により、通信装置は両方の認証段階、PPPプロトコルの切断を行い、インターネットプロトコルトラフィックをルーティン

グする。

本発明の別の実施例では、通信装置20は移動又は陸上から発信されたデータ呼出に対して直通PSTN (Public Switched Telephone Network) 接続を可能に

する。この実施例では、通信シャシ20、例えば前述のトータル・コントロール・ネットワーク・エンタープライズ・ハブは、必要とされるモデムと電話回線インタフェース及びこれらの機能を実行するための処理回路を含む。この実施例は、インターネットサービスプロトコルが市内の電話会社である場合に特に有利である。本発明によるインターネットアクセス方法によれば、通信装置20は、移動データユーザから移動発信データ呼出の最中に発せられたATDコマンド内の被呼出番号を抽出ないし取り出す。ほとんどの呼出番号の場合、通信装置20は呼出を通常のPSTNモデム呼出として処理する。しかし、呼出番号がインターネットアクセスに関連付けられている場合、通信シャシ20は呼び出された番号 (ISPのバックボーンネットワーク26上、又は通信シャシ20に専用線36、42又はその他のネットワークを介して接続されている) に関連付けられた認証サーバ32Aにおいて第1の認証段階を実行する。認証サーバ32Aは、認証サーバ32Aの管轄下にあるインターネット22又はネットワーク24をアクセスすることが遠隔ユーザに許可されているかどうかを判断する。

図2は図1の通信シャシ又はネットワークアクセスサーバ20の好適な形態を簡略化して示した機能ブロック図である。この通信シャシ又はネットワークアクセスサーバ20はワイヤレスユーザのみならず、公衆

交換電話ネットワークからダイヤルしているユーザにもサービスを提供することができる。そのため、シャシは本発明の実施には必要とされない機能を含み、PSTNが可能にされている本発明の特定の実施例において必要とされる別の機能を実行する。図2のネットワークアクセスサーバ20は基本的に、出願人の譲受人から入手可能な市販製品であるトータル・コントロール・ネットワーク・エンタープライズ・ハブの現行モデルのアーキテクチャと設計を一にする。業界のそ

の他のメーカーの統合アクセスサーバを適当に修正して本発明の機能を得ることも可能であり、この明細書に記載された実施例のみに本発明が限定されていると解すべきではない。

ネットワークアクセスサーバ20は電話ネットワークインタフェースカード50を含む。この電話ネットワークインタフェースカード50は、T1、E1及びISDN基本レートインタフェース(PRI)回線、及びフレームリレー回線等の時分割多重デジタル電話回線に接続されている。ネットワークインタフェースカードは、無線円滑ユーザからのデジタルデータを、フレームリレー回線FR上のワイヤレスサービススイッチを介して受け取る。インタフェースカード50は電話回線を物理的に受け入れるためのコネクタを有する。該カード50はさらに、入力信号からクロック信号とデータを取り出し、出力及び入力データ流に

多重化及び多重分離を施すCSUを有し、それによって呼出をキャリアの時間スロット内に配置する。カード50は入力電話信号をNIC/NAC (network interface card/network application card) バス54を介してT1/E1/ISDN PRI/ネットワークアプリケーションカード56に送信する。アプリケーションカード56は、取り出された電話回線データに対してフレーミングを供給することにより、フレームリレー時分割多重データ、T1 DS0チャンネルデータ、又はISDN PRI信号に含まれたISDN 2B+Dチャンネルデータを取り出し、その後時間/空間スイッチを利用して、チャンネルデータを、シャシ内バスミッドプレーン52の一部である時分割多重バス60上の時間スロットに切り換える。

入力信号がワイヤレスサービス中央オフィスからのものであり、フレームリレー回線上でサーバに到着したものである場合、チャンネルデータは通常モデムにおいて行われる信号変換処理は必要とせず、TDMバス60を介してルーティング及びLAN/WANインタフェースカード62にルーティングされる。トータル・コントロール・エンタープライズ・ネットワーク・ハブでは、このカード62は“エッジサーバ (EdgeServer)” カードとして公知であり、Ascend社、Livingston社その他のメーカーのネットワークアクセス装置も同様のインタフェースを有

している。エッジサーバカ

ード62は、TCP/IPプロトコルに従ってデータパケットを組み入れた一対のミュンヘンチップを有し、LAN/WANインタフェース又はトータルサーバを介して直接目的地に送信する。

公衆交換電話ネットワークに接続されたユーザから発せられた呼出であり、信号変換が必要な場合、TDMバス60は呼出をマルチ・モデム・モジュール内のモデム又はカード64に向ける。内部シャシバス52はさらに高速並列バス58を有し、該バス58は、復調/信号変換後のデータをエッジサーバカード62内のルーティングエンジンに伝送するために、カード64内のモデムをエッジサーバカード62に接続する。複数のアナログネットワークインタフェースカード63が、モデムを直列インタフェース65に接続するために設けられている。

電話回線インタフェースカード50とアプリケーションカード56、モデムカード63、64、内部シャシバスコンプレックス52（TDMバス60及び並列バス58を含む）、並びにエッジサーバカード62のコンピュータネットワークインタフェース66は、上述のBaum他の米国特許第5577105号：「データ通信用の電話呼出交換及びルーティング方法」に、また、Walsh他の米国特許第5528595号：「モデム入出力信号処理方法」に詳細にそれぞれの構成回路と動作が記載されている。好適な内部シャシバスの詳

細な構造はPanzarella他の米国特許第5416776号「モデムバックプレーン技術」に開示されている。この特許は3COM社に譲受されており、参照として本明細書に引用する。マネージメントカードによるシャシの運営はPanzarella他の米国特許第5436614号「モデム管理技術」にも詳細に説明されている。この米国特許もまた3COM社に譲受されており、参照として本願明細書に引用する。

エッジサーバカード62は汎用計算プラットフォーム70を含み、該プラットフォーム70により市販のスタンドアローン型又はシェアウェアによるオペレーティ

ングシステム（ウィンドウズNT等）が駆動される。カード62は本願明細書に参照として引用する、William Verthein他の特許出願第 号に詳細に記載されている。

電話回線インタフェース、アプリケーションカード、モデムカード、管理カード（図示しない）、及びカード62のコンピュータネットワークインタフェース66は公知の製品内に存在し、又は公知の文献に記載されており、当業者であればそのような回路（ないしは同等物）を如何にして設計・製作するかは明らかであるので、通信アクセスシャシ10のこれら構成要素の説明は省略する。また、通信シャシ10のアーキテクチャ又は設計に関する詳細も特に重要でない。

エッジサーバカード62はTDMインタフェース7

2を有し、該インタフェースはフレームリレーFR回線からTDMバス60を介してチャネルデータを受け取る。計算プラットフォーム70は市販のIBM互換機パソコン、それに付随する統合中央処理ユニット74、及びキーボード、フロッピーディスク、モニタ並びにマウス用の周辺機器インタフェースから構成される。計算プラットフォームはまた、内部記憶用ハードディスクドライブ76を含む。計算プラットフォームはさらにパケットアセンブリ・逆アセンブリ回路78を含み、それによってモデムモジュール64内のモデムからのデータパケットが、汎用計算プラットフォーム70の使い易いフォーマットに組み立てられる。汎用計算プラットフォームはNIC/NACバス接続を介して通常のネットワークインタフェース66とも通信する。計算プラットフォームはまた、第2のISAバス82を介して外部記憶拡張バスインタフェース84とも通信を行う。該インタフェース84は外部ディスクドライブ又はその他適当な記憶装置に接続され、通信シャシ20の記憶容量を増大させるために使用される。好適な実施例では、後述するような通信シャシ20内でのトンネリング及び認証機能を駆動するためのソフトウェアは、エッジサーバカード62内の汎用計算プラットフォーム70内にロードされている。

上述のように、図2の通信シャシによるアーキテクチャ及び機能は、ワイヤレスネットワーク上の遠隔

ユーザをISPバックボーン、企業ネットワーク又はインターネットに接続するために通常必要とされる機能以上の機能を提供する。図2Aはモデムを有しない別の装置の略図である。この装置は、通信装置用のPSTN切断機能が設けられていない実施例において用いると好適である。図2Aの実施例では、回線インタフェースユニット、デマルチプレクス回路及びフレーミング回路を有したフレームリレーインタフェース100が1つのモジュール内に設けられている。インタフェース100はチャネルデータをTDMバスコンプレックス内において時間スロット上に配置する。TDMバスコンプレックス102はインタフェース100をLAN/WANインタフェース104に接続する。LAN/WANインタフェース104は好適には一般的なイーサネット又はその他一般のインタフェースから構成される。後者の場合は、呼びルーティング、認証、トンネリングその他本願明細書に記載の機能を実行するソフトウェアがロードされた汎用計算プラットフォームにより修整される。

図1、2及び2Aから、デジタルデータ源12をコンピュータネットワーク24、22（企業内プライベートネットワーク、インターネット、ワールド・ワイド・ウェブ等）に接続する方法が開示されていることが明らかであろう。デジタルデータ源12はデジタルデータを発生し、無線伝送媒体を介して無線サ

ーバキャリアと通信を行う。キャリアはデジタルデータを多重化し、回線FR等の高速デジタル電話回線に送る。この方法は以下のステップを有する。

（1）ネットワークアクセスサーバ又は通信シャシ20においてデジタルデータ受け取り、該デジタルデータから少なくとも（a）デジタルデータ源12により呼び出された電話番号、又は（b）デジタルデータ源と関連付けられた電話番号、を有するネットワークアクセス認証データを抽出する。

（2）認証データを、通信装置20に接続されたローカルエリア又はワイドエリアコンピュータネットワークを介して、コンピュータネットワーク24又は22用のネットワーク認証サーバ32A又は32Bに送信する。ネットワーク認証サーバはローカルエリア又はワイドエリアコンピュータネットワーク26を介して通信シャシ20と結合されている。

(3) 認証サーバ32Aにおいて、送信されてきた認証データに基づいて、遠隔ユーザがコンピュータネットワーク22ないし24にアクセスすることが許可されているかどうかを判断する。認証サーバ32Aは通信シャーシ20に判断ステップの結果をし、該判断ステップの結果が肯定であるならば、データ源12に対してコンピュータネットワーク24へのアクセスを許可する。

この方法はさらに、ローカルエリア又はワイドエリ

アネットワーク26を介して通信シャーシ20に結合されたトンネリングサーバ30又は34を識別し、デジタルデータ源12からのデジタルデータをトンネリングサーバ30にルーティングしてコンピュータネットワーク24に対するアクセスを与えるステップを含むことができる。前記通信シャーシ20はデジタルデータ源12に対して、コンピュータネットワークへのアクセスを与える。トンネリングサーバの識別は、好適な実施例では、発生した呼び出しから抽出された認証データ（すなわちダイヤルされた番号及びダイヤルした側の番号）により決定される。この実施例では、認証サーバ32A又は32B内で、通信装置20とトンネリングサーバ30間でデジタルデータをトンネリングする際に使用される、データ源12用トンネリングプロトコルを決定することによっても本発明を実施できる。この決定ステップは例えば、ソフトウェアルックアップテーブル内で、遠隔ユーザ12（遠隔ユーザ12の電話番号により識別される）と関連付けられたトンネリングサーバ及び必要なプロトコルを見つけ出すことによっても実行可能である。デジタル電話はトンネリングサーバを介してトンネリングプロトコルに従ってルーティングされる。本発明の好適な実施例では、PPTP又はTELNETプロトコルが使用される。

好適な実施例では、図2の通信シャーシ20は、T1

/E1 ISDNインタフェース50/56を介しての公衆交換電話ネットワークに対するアクセスも供給する。通信シャーシ20は遠隔ユーザ12からのデジタルデータをそのデータの目的地にルーティングする。このようにして、通信シャーシ20はコンピュータネットワーク22と24に対する直接的ネットワークアクセス

を供給するだけでなく、シャーシ内のモデムを介して信号変調を行い、呼び出しを電話ネットワークを介して遠隔端末、例えば図1のコンピュータ13に送信可能にする。通信シャーシ20がどのようにしてPSTNコネクティビティを与えるかは公知であり、前述のWalsh他の特許に記載されている。

本発明の好適なネットワークアクセス実施例において、第2段階の認証ルーチンにより、遠隔ユーザの指定ネットワークへのアクセスが許可されていることが確認される。これは、PAPやCHAPルーチン等のパスワード認証プロシーダを、

(1) トンネリングサーバ30又は(2) 認証サーバ32Aと遠隔ユーザの間で実行することにより、又は(3) 認証サーバ32Aとトンネリングサーバ30/34間で実行することにより、第2レベルの認証を行うことにより達成される。これらのルーチンはいずれも公知である。

本発明の1つの実施例においては、高速電話回線を介してユーザ12から電話呼び出しを受け取るよう構成されたネットワークアクセスサーバ又は通信シャー

シ20を有したインターネットサービスプロバイダによる使用に適したインターネットアクセス方法が開示される。この方法は以下のステップを有する。

(1) ネットワークアクセスサーバ20を、ローカル又はワイドエリアネットワーク26を介して認証サーバ(32A又は32B等)に接続する。

(2) ユーザ12により発生された呼び出しから、少なくとも(a) ユーザの呼び出した電話番号、又は

(b) ユーザと関連付けられた電話番号、を含むネットワークアクセス認証データを抽出する。

(3) 発生呼び出しから抽出したネットワーク認証データを認証サーバ32A又は32Bにルーティングし、ネットワークアクセス認証データに基づいてユーザを認証する。

(4) ネットワークアクセスをユーザに与えるためのトンネリングサーバ(例えば34)を識別し、通信シャーシ20に該トンネリングサーバを通知する。

(5) 通信シャーシ20からのデジタルデータをトンネリングサーバ34にトンネリングする。

(6) 前記デジタルデータを前記トンネリングサーバによりインターネットに送る。

好適な実施例では、この方法は、トンネリングステップのためにユーザに対するトンネリングプロトコルを識別するプロセスにより達成される。例えば、認証サーバ32A又は32B又は40により、遠隔ユーザ

の特徴、指定されたトンネリングサーバの必要とする条件、その他に従って、ユーザを特定のトンネリングプロトコル(PPTP又はTELNET)に関連付けることができる。そのような情報は典型的には認証サーバ32Aのメモリ内に記憶されている。

さらに、本発明はインターネットサービスプロバイダシステムを無線インターネットユーザとして想定している。このインターネットサービスプロバイダはネットワークアクセスサーバ20(図2)を有し、該サーバは以下の構成要素を有している。

(1) 無線インターネットユーザからの呼出を受ける高速デジタル電話回線FRインタフェースと、前記無線インターネットユーザに関連付けられたデジタルデータをインターネットに送出するためのインターネットゲートウェイ(図2のWANインタフェース66等)。

(2) 通信媒体26を介してネットワークアクセスサーバ20に結合されたインターネットアクセス認証サーバ(32A等)。該認証サーバは無線インターネットユーザに関連付けられたデジタルデータから抽出されたインターネットアクセス認証データに応じて動作する。

(3) 認証サーバ32Aはさらに、インターネットアクセス認証データに基づいて、無線インターネットユーザ12がインターネットにアクセスすることが許

可されているかどうかを判断するためのメモリを備える。インターネット認証サーバは認証応答をネットワークアクセスサーバ20に送出する。ネットワークアクセスサーバ20は認証サーバからの認証応答に応じて、無線インターネットユーザに対してインターネットへのアクセスを認めるか、又は該無線インターネッ

トユーザからの呼出に関してその他の何らかの動作を行う。例えば、インターネットサービスプロバイダは認証照会を、第2のインターネットサービスプロバイダにより運営されている他の認証サーバ（図1の40等）に転送し、前記ユーザが第2のインターネットサービスプロバイダのクライアントであるかどうかを確かめる。

本発明の好適な実施例の実施の詳細に関しては、図3～11を参照して説明する。

図3は遠隔ユーザ12、通信シャシ20、インターネットサービスプロバイダバックボーンネットワーク26内のルータ（図示しない）、及び図1の指定されたトンネリングサーバ30又は34間のトンネルインタフェースのプロトコルスタックとアーキテクチャを図示したものである。図3では、番号L1とL2は下位プロトコル（データリンク層等）を示している。IPはインターネットプロトコルを示す。PPPはポイントツーポイントプロトコルを示す。TCPは伝送制御プロトコルを示す。非同期（Async）という用語は遠隔

ユーザ12と関連付けることのできる非同期プロトコルを示し、TELNETプロトコルは通信シャシ20とトンネリングサーバ内で非同期通信のために用いられる。図から明らかなように、通信シャシ20がトンネリングサーバと通信する際には、IP及び下位プロトコル上で動作するPPTP又はTELNETを使用する。

図4に示すように、通信シャシ20の通信相手である認証サーバ（32A等）はRADIUSを実行し、UDP/IPプロトコルスタックを介して認証と課金を行う。図4は、ネットワークアクセスサーバ又は通信シャシ20と図1の認証サーバ32A間の認証・課金インタフェース用のプロトコルを示す。UDPは、インターネットプロトコル（IP）の上位に位置するコネクションレス型プロトコルである。

通信シャシ20がインターネット22と通信する場合、トンネリングプロトコルはない。図5に示されているのは、遠隔ダイアルユーザと、該ユーザを目的地端末装置に接続するルータ間の非トンネルインタフェース用プロトコルスタック

である。

図6は、本発明の好適な実施例における呼び出し受入シナリオにおけるPPTPプロトコルトンネリングの呼出フローを示す。図6では、プロセスは素00における呼出の発生から始まる。呼出は特定の目的地電話番号（図示の例では1-800-123-4567）に関連付けられ

ている。

ステップ102では、通信シャシが、ローカルエリアネットワークを介して通信シャシに接続されている認証サーバ（32A又は32B等）に対して第1段階の認証アクセスルーチンを開始する。この認証要求は認証サーバに転送されるソフトウェア構造であり、以下の情報のためのフィールドを含む。（1）遠隔ユーザに関連付けられた電話番号（これは公知の呼出人識別技術又は前記Baum他の特許に記載の方法に従って検知される）；（2）公知の方法により取り出されるダイヤルされた電話番号；（3）通信シャシ20内の呼出に関連付けられた特定のチャンネルないしポート番号すなわちポートID；及び（4）通信シャシ20のIPアドレス。

ステップ104では、認証サーバ32Aは通信シャシ20にアクセス応答メッセージを送る。ユーザが、認証サーバ32Aの管轄下にあるネットワークに対してアクセス許可されていれば、前記メッセージは、PPTPが適切なトンネリングプロトコルであるという確認と、トンネリングサーバのIPアドレスの確認と、呼出を受けるトンネリングサーバのポート番号を含む。遠隔ユーザがアクセス許可されていない場合、以下に説明するような図8のプロシージャが使用される。

ステップ106では、通信シャシ20は発生呼出要

求（Incoming-Call-Request）メッセージをトンネリングサーバ34に送出する。このメッセージは遠隔ユーザのダイヤル番号の識別、ダイヤルされた電話番号、及びサブアドレスを含む。ステップ108では、トンネリングサーバ34が呼出を受入可能であれば、発生呼出応答（Incoming-Call-Reply）メッセージ、例

例えばアクセス照会の結果が肯定であれば「コネクト」を送出する。トンネリングサーバが呼出を受け取れない場合は、図9のプロシージャが使用される。

ステップ110では、トンネリングサーバ34から「コネクト」メッセージが受け取られた場合、通信シャシ20は呼出受入メッセージをフレームリレー回線FR及びワイヤレスネットワークを介して遠隔ユーザに送出する。そして入力呼出接続メッセージがステップ112において通信シャシ20からトンネリングサーバ34に中継される。

ステップ114では、好適には（つまりオプションとして）第2段階の認証プロシージャが実施される。ステップ116、118、120、122、124及び126は図6から自明であり、公知のPAP及びCHAPパスワード認証プロトコルの一部であり、当業者には明らかである。

ステップ128では、仮にパスワード認証を通過したとして、トンネリングサーバ34から遠隔ユーザ12に対して、通信シャシ20を介して遠隔ユーザ12

とトンネリングサーバ34間にPPPリンクが確立された旨のメッセージが送られる。この時点で、遠隔ユーザとネットワーク22又は24上のホスト間での、インターネットプロトコルに従ったデータパケットの伝送が完了する。

図7は本発明の好適な実施例における、呼出受入シナリオのためのTELNETプロトコルトンネリングの呼出フローを示す。このプロセスは概して図6に記載されたものと同様であり、図から自明である。TELNETセッションの確立の為には、通信シャシ20とトンネリングサーバ34間におけるハンドシェーキング及びパラメタ折衝が必要である。これは、ステップ130及び132に示されている。PAP等のログインプロトコルを使用した、認証の第2段階が図示のように実行される。トンネリングサーバ34からダイアルユーザ12に対してログイン受入メッセージが送られると、通信サーバ20とトンネリングサーバ34を介して、遠隔ユーザ12とコンピュータネットワーク（インターネット等）上のホスト間で非同期伝送が実行される。

アクセス認証の第1段階で、認証サーバが、該認証サーバの管轄下にある指定されたネットワークへのアクセスが遠隔ユーザに許可されていない（例えば、遠

隔ユーザの電話番号が、シャシ20を運営しているインターネットサービスプロバイダのインターネットク

ライアントデータベースに合致しないため)と判断することもある。このシナリオに対処する好適な方法が図8に示されている。すなわち図8は認証失敗シナリオにおける呼出フローを示す。認証サーバ32Aが、遠隔ユーザが許可されていないと判断すれば、認証サーバ32から通信シャシ20に対してアクセス拒否メッセージが送られる。このメッセージは、アクセス拒否の理由を示したフィールドを含むことができる。そのような理由は例えばダイヤルした電話番号が間違っている、ISPがユーザの電話番号を認識しない、ユーザの毎月の使用料の支払いが遅れている、認証サーバが使用中止になっている、等である。通信シャシ20はその場合、遠隔ユーザ12に対して後ほどトライし直すようメッセージを送るか、該呼出をPSTN/モデム呼出として扱い呼出をPSTNシステム上でルーティングするか、又は該呼出を拒絶して切断シーケンスを開始する。

さらには認証サーバ32Aがネットワークへのアクセスを許可するが、トンネリングサーバ30又は34が遠隔ユーザ12と目標ネットワーク22ないし24間でのデータ転送のための機構として機能出来ないという状況が考えられる。図9はトンネリングサーバアクセス拒絶シナリオにおける呼出フローを示す。第1ステップ100、102、104及び106は図6と共通である。トンネリングサーバ34が呼出を処理で

きない場合、トンネリングサーバ30ないし34は通信シャシ20に、入力呼出応答を、呼出を受け入れられない旨のメッセージないしフィールドと共に送る。この時点で、通信シャシ20は遠隔ユーザ12に対して後ほどトライし直す旨のメッセージを送るか、該呼出をPSTN/モデム呼出として扱い電話システム上でルーティングするか、又は単に呼び出しを拒絶する。

前記図6と7に関連して説明した認証の第2段階において、ユーザがパスワード認証プロシージャにおいて失敗することもある。図10はPPTPプロトコルにおける認証失敗シナリオにおける呼出フローを示す。PPTPプロトコルでは

、ログインパスワード認証プロシージャが、ネットワークアクセス認証プロシージャの第2段階として実行される。ステップ140では、アクセス拒絶メッセージが認証サーバ32Aからトンネリングサーバ30/34に対して送出される。この時点(ステップ142)で、トンネリングサーバはログイン拒絶メッセージを遠隔ユーザ12に送る。

図11は、ログインパスワード認証プロシージャが、ネットワークアクセス認証プロシージャの第2段階として実行される、TELNET用認証失敗シナリオにおける呼出フローを示す。このプロセスは基本的に前記のプロセスと同様に進行する。

PPTP及びTELNETトンネリング、課金及び

第1・第2という2段階の認証の好適な実施例を以下に詳細に説明する。

プロトコルインタフェース

通信シャシ20はダイヤルユーザ(無線端末)、MSC、ルータ、認証サーバ、及びトンネリングサーバとインタフェースする。本明細書では認証サーバとトンネリングサーバに対する通信シャシインタフェースについてのみ説明する。その他のインタフェースは当業者には明らかである。

PPTPトンネリング

PPTPトンネリングは、認証の第1段階中のRADIUS アクセス応答メッセージからのログインサービス属性に基づいて使用可能にされる。プロトコルがPPTP値(RFC2058ではTBD)を有していれば、PPTPトンネリングが通信シャシとトンネリングサーバ間に設定され、呼出人からの以後のトラフィックがトンネルされる。

通信シャシゲートウェイはPPTP RFC内のPAC(PPTPアクセスコンセントレータ)と同等であり、トンネリングサーバはPPTP RFC内のPNS(PPTPネットワークサーバ)と同等である。以下のPPTPの説明では、PAC及びPNSという用語を使用する。

個々の構成されたPPTP PAC-PNS対に関して、PAC(通信シャシ)とPNS(トンネリングサ

一バ) 間のインタフェースは2つの並列要素から構成される。すなわち、

1. TCP上で動作する制御接続
2. 個々の対間のユーザセッションのためのカプセル化されたPPPパケットを伝送するIPトンネル。

PPTP制御接続

PACとPNS間でPPPトンネリングを生じさせる前に、それらの間で制御接続が確立される必要がある。制御接続は標準的なTCPセッションであり、その上をPPTP呼出制御及び管理情報が通過する。制御セッションはPPTPトンネルを介してトンネリングされているセッションと論理的に関連付けられているが、別個のセッションである。

PPTPトンネル接続

PPTPはそれぞれの通信しているPAC-PNS対においてトンネルを確立することを必要とする。トンネルはPAC-PNS対に関わるセッションのための全てのユーザセッションPPPパケットを伝送するために使用される。GREヘッダ内にあるキーにより、どのセッションに特定のPPPパケットが属するかを示す。このようにして、PPPパケットは所与のPAC-PNS対間の単一のトンネル上で多重化及び逆多重化される。キーフィールドにおいて使用する値は

、制御接続上で実行される呼び出し確立プロシージャによって確立される。

PPTP制御接続メッセージ

制御接続管理メッセージ:

以下のメッセージから構成される。

- ・制御接続開始要求
- ・制御接続開始応答
- ・制御接続停止要求
- ・制御接続停止応答
- ・エコー要求
- ・エコー応答

呼び管理メッセージ:

以下のメッセージから構成される。

- ・出力呼び要求（この時点ではサポート無し）
- ・出力呼び応答（この時点ではサポート無し）
- ・入力呼び要求
- ・入力呼び応答
- ・入力呼び接続完了
- ・呼びクリア要求
- ・呼び切断通知

エラー報告

- ・WANエラー通知

PPPセッション制御

- ・セットリンク情報

PPTPトンネル接続メッセージ

PPTPデータPDU：

PPPフレームはそれぞれGRE（Generic Routing Encapsulation Header；汎用ルーティングカプセル化ヘッダ）内でカプセル化されている。GREは参照として本願明細書に引用するコメント要求（RFC1701、1994年10月）に記載されている。

Telnet トンネリング

PPTPとL2TPプロトコルは非同期トラフィックをトンネリングするようには設計されていない。同期トラフィックはTelnetプロトコル（RFC854を参照）によりトンネリングされる。

Telnetの実施はECHO、linemode、binary、SUPPRESS GO AHEAD等のTelnetコマンド及びオプションを支援しなければならない。トンネリングサーバは任意のTelnetセッションにおいてTelnet接続の最中に1つのモードから別のモードへ切換を要求出来なければならない。この切換は例えばECHOからNO ECHO、linemodeを経てbinary伝送へという具合である。

さらに、通信シャシゲートウェ

イにおいてはエスケープ機能を使用禁止にして、ダイアルユーザが通信シャシゲートウェイ上のローカルモードに入ることを防止する必要がある。

T e l n e t トンネリングは、第1段階認証中に、R A D I U S アクセス応答メッセージからのログインサービス特性に基づいて使用可能にされる。ログインサービス属性が値T e l n e t を有していれば、通信シャシとトンネリングサーバ間にT e l n e t が設定され、発呼者からの以後のトラフィックがトンネリングされる。

R A D I U S 認証インタフェース

2段階の認証が使用される。認証の第1段階は発呼者番号、被呼番号、及び通信シャシI Pアドレスに基づいて行われる。認証の第2段階は、ユーザ名、パスワード、及び／又は呼び掛け・応答（オプション）に基づいて行われる。

ここでは第1と第2段階両方のR A D I U S 認証のやりとりを説明する。トンネリングオプションの何れか1つを使用する場合、エンドユーザ認証は、通信シャシに対して透過性（transparent）である認証の第2段階においてトンネリングサーバにより行われる。非トンネリングインターネットアクセスの場合、通信シャシは認証の両方の段階を行う（第1段階は省くこともオプションとして可能である）。

以下の一般的動作がR A D I U S インタフェースに該当する。

1. この文書はI E T F R A D I U S 認証R F C 2 0 5 8に従っている。認証サーバはR F Cに規定されたR A D I U S サーバ機能を提供する。通信シャシ及びトンネリングサーバはR A D I U S クライアント機能を実施する。

2. 通信シャシは少なくとも2つの認証サーバを個々の特別インターネットアクセス被呼番号に関連付けることができるものとする。これら2つ（又はそれ以上）の認証サーバは第1及び第2のR A D I U S 認証サーバ機能を提供する。それぞれの認証サーバは構成可能なサーバI Pアドレス及びUDPポートにより識別可能である。複数のインターネットアクセス被呼番号が認証サーバを共有する場合もあるし、そうでない場合もある。

3. R A D I U S 共有秘密（1～15文字）はサーバ毎に行政的に構成される

。この明細書では共有された秘密が通信シャシゲートウェイとRADIUSノード（認証サーバ）間でどのように管理されるかは論じないが、そのような詳細は当業者には明らかである。

4. 通信シャシゲートウェイは再送信アルゴリズムを実施し、それによってアクセス要求の消失に対処できる。構成可能な再送信カウンタは、特定のインターネットアクセス呼出番号に対する認証サーバがいつ動

作停止中であるかを判断し、停止中は通信シャシはオプションとして、標準的なPSTN/モデムアクセスプロシージャに従う。

認証インタフェース第1段階

アクセス要求メッセージ：

RADIUSアクセス要求メッセージは通信シャシ20によりRADIUSサーバ（認証サーバ32A）に送られ、入力呼出が示される。以下は、メッセージと共に送られる属性のリストである。

- ・ユーザ名：全ての入力呼出に対してVENDORIDに設定。
- ・ユーザパスワード：ゼロに設定。
- ・NAS-IPアドレス：通信シャシのIPアドレスに設定。
- ・NASポート：通信シャシ上の発呼者に関連付けることのできるポート番号又はその他の識別子
- ・被呼局ID：被呼者の番号又は電話識別子。これは発呼者の希望するサービスを識別するために使用される。
- ・発呼局ID：発呼者の番号又は電話識別子。これは認証第1段階に使用することもできる。
- ・NASポートタイプ：通信シャシスイッチ上でユーザにより使用されるポートの種類を特定する。（RFC2058における無線アクセス用TBD値）

アクセス受入メッセージ

RADIUSアクセス受入メッセージはRADIUS（認証サーバ）により通信シャシ20に送られ、特定のサービスに対する入力呼出の受入が示される。以

下は、認証サーバから通信シャシに送られる属性のリストである。

- ・サービスタイプ：PPTP又はTelnetトンネリングに対しては1（ログイン）に設定。PPPを使用する非トンネリングインターネットアクセスに対しては2（フレーム化）に設定。

- ・ログインサービス：0-Telnet又はTBD-PPTPに設定。サービスタイプ属性が2（フレーム化）に設定されている場合は使用されない属性。

- ・ログインIPホスト：発呼者が接続されるべきトンネリングサーバのIPアドレス。サービスタイプ属性が2（フレーム化）に設定されている場合、使用されない属性。

- ・ログインTCPポート：発呼者が接続されるべきトンネリングサーバ上のTCPポート。サービスタイプが2（フレーム化）に設定されていれば使用されない属性。

- ・応答メッセージ：Telnetユーザに対してのみ送られるオプション。通信シャシはこの属性を非同期ストリングとして、トンネリングサービスに対するT

ELNETトンネリングを完了する前に転送する必要がある。

- ・フレーム化プロトコル：サービスタイプ属性が2（フレーム化）に設定されていれば、1に設定される。サービスタイプが1（ログイン）に設定されていれば使用されない属性。

アクセス拒絶メッセージ

RADIUSアクセス拒絶メッセージはRADIUSにより通信シャシに送られ、特定のサービスに対する入力呼出を否定する。通信シャシはこのメッセージを受け取ると、通常のPSTN/モデムプロシージャに進む。応答メッセージ属性がアクセス拒絶メッセージに含まれていれば、通信シャシはASCIIストリングメッセージをユーザに送る。以下の属性はオプションとしてRADIUSから通信シャシに送ることができる。

- ・応答メッセージ：Telnetユーザのみに送られるオプション。通信シャシは、通常のPSTN/モデムプロシージャに進行する前に、この属性の内容を

非同期ストリングとして発呼者に送る必要がある。

第2段階認証インタフェース

ここでは通信シャシと、非トンネリングインターネットアクセスオプションを使用した認証サーバ間の第

2段階認証メッセージを特定する。さらに、トンネリングサーバ（RADIUSクライアント）と認証サーバ（RADIUSサーバ）間の、何れかのトンネリングオプションに基づいた、考えられる第2段階認証のやりとりの例を説明する。

アクセス要求メッセージ

RADIUSアクセス要求メッセージは通信シャシからRADIUSに送られ、入力呼出が示される。以下のリストはメッセージと共に送られる属性である。

- ・ユーザ名：この属性は認証を希望しているダイアルインユーザの名前を示す。
- ・ユーザパスワード：この属性は認証を希望しているダイアルインユーザのパスワード、又はアクセスチャレンジ後のユーザの入力を示す。
- ・NAS-IPアドレス：通信シャシのIPアドレスに設定。
- ・NAS-Port：通信シャシ上で発呼者と関連付けることのできるポート番号ないしはその他の識別子。
- ・サービスタイプ：2に設定（フレーム化）。
- ・フレーム化プロトコル：1に設定（PPP）
- ・フレーム化IPアドレス：ダイアルインユーザ12はオプションとしてローカルスタチック構成IPアドレスを要求できる。このIPアドレスは、アクセス

受入メッセージ内に含まれた同様の属性により書き換えることができる。

アクセス受入メッセージ

RADIUS受入メッセージはRADIUSにより通信シャシに送られ、特定のサービスに対する入力呼出の受入が示される。ダイアルユーザはまた、このメッセージによりIPアドレスを割り当てられる。以下の属性はRADIUSから通信シャシに送られる。

・フレーム化IPアドレス：この属性は、ユーザに割り当てるIPアドレスを示す。

アクセス拒絶メッセージ

RADIUSアクセス拒絶メッセージはRADIUS（認証サーバ）により通信シャシに送られ、入力呼出に対して特定のサービスが拒絶される。通信シャシはこのメッセージを受け取ると、要求されたサービスが利用不可能であることを示し、ユーザ接続を切断する。

アクセスチャレンジメッセージ

RADIUSアクセスチャレンジメッセージはオプションとしてRADIUSにより通信シャシに送られ、チャレンジ/レスポンス認証プロシージャをRFC 2058に従って実行する。

RADIUS課金インタフェース

通信シャシとトンネリングサーバの両方は、RFC 2059に規定されたようにRADIUS課金クライアント機能を実施する。課金サーバが、呼出を制御する認証サーバと関連付けられていれば、それぞれのRADIUS課金クライアントは以下のRADIUS課金メッセージをここに記載のように送出する。

通信シャシ及びトンネリングサーバからの課金クライアントは、RADIUS認証サーバからアクセス受入メッセージを受け取ると、課金スタートメッセージを送る。

呼出が一旦放棄、クリア、ないし切断されると、課金クライアントは課金ストップメッセージをRADIUS 課金サーバに送る。

課金スタートメッセージはRADIUS課金要求により、課金ステータス値を1に設定されて、送信される。課金ストップメッセージはRADIUS課金要求メッセージにより、課金ステータスタイプ値を2に設定されて送信される。

課金要求メッセージ

課金要求パケットはクライアントからRADIUS課金サーバに送られ、ユーザに対して供給されたサービスに対する課金を供給するための情報を伝送する。

以下は、メッセージと共に送ることのできる課金関連属性の一部である。

- ・課金ステータスタイプ：この属性は、この課金要求がユーザサービスの始まり（スタート）なのか、又は終わり（ストップ）なのかを示す。
- ・課金遅延時間：このお属性は、クライアントが何秒間この記録を送ろうとしていたかを示す。この属性をサーバへの到着時間から抽出することにより、課金要求を発生しているイベントのおよその時間を知ることができる。
- ・課金入力オクテット：この属性は、このサービスが供給されてからいくつのオクテットがポートから受け取られたかを示し、課金ステータスタイプがストップに設定されている課金要求記録内にのみ存在する。
- ・課金出力オクテット：この属性はこのサービスを供給し始めてからいくつのオクテットが通信シャシに送られたかを示し、課金ステータスタイプがストップに設定されている課金要求記録内にのみ存在する。
- ・課金セッションID：この属性は、個別の課金IDであり、ログファイルにおいてスタートとストップ記録のマッチングを容易にする。任意のスタート・ストップ記録は同一の課金セッションIDを有していなければならない。課金セッションIDはプリント可能なASCIIストリングであることが推奨される。
- ・課金認証：この属性は、課金要求に含めることが

でき、ユーザがいかに認証されたか、すなわちRADIUSによってか、送り出し側によってか、又はその他のリモート認証プロトコルによってかを示す。認証なしにサービスを提供されたユーザは課金記録を発生しないはずである。

・課金セッション時間：この属性は、ユーザが何秒間サービスを受け取ったかを示し、課金ステータスタイプがストップに設定されている課金要求記録においてのみ存在し得る。

・課金入力パケット：この属性はフレーム化ユーザに対してサービスが供給されて以来ポートから何個のパケットが受け取られたかを示し、課金ステータスタイプがストップに設定されている課金要求記録においてのみ存在し得る。

・課金出力パケット：この属性はフレーム化ユーザに対してサービスが供給されて以来ポートに対して何個のパケットが送られたかを示し、課金ステータスタイ

ブがストップに設定されている課金要求記録においてのみ存在し得る。

・課金中止原因：この属性は、セッションがどのように中止されたかを示し、課金ステータスタイプがストップに設定されている課金要求記録においてのみ存在し得る。

課金応答メッセージ

課金要求を受け取ると、RADIUS課金サーバは課金応答メッセージにより、課金パケットの記録に成功したかどうかに関して応答しなければならない。課金パケットの記録に失敗した場合は送信しない。

グロッサリー

用語及び略語

CDMA (Code Division Multiple Acces ; 符号分割多重接続)

移動電話及びPCSスペクトラムにおけるデジタル音声及びデータワイヤレス通信のための北米基準。ユーザを無線インタフェース上で多重化するための技術。

インターネットプロトコル (IP)

ユーザデータグラムをインターネットを介して不信頼性・コネクションレス伝送するための仕組みを定義する。

IWP-IP

通信シャシは、TDMAないしCDMA移動電話に接続された端末装置と、PSTN及びインターネットネットワークに接続された端末装置とを協働させるための機能を供給する。

第2レイヤトンネリングプロトコル (L2TP)

PPPのリンクレイヤプロトコルのトンネリングを可能にするために定義されたプロトコル。現在のところ草稿RFC段階であるが、標準として採用される見通しである。

移動交換センタ (MSC)

移動電話又はPCSワイヤレス遠隔通信ネットワーク内のネットワーク要素で

あり、ワイヤレスユーザに対してPSTNコネクティビティ、制御機能、及び交換機能を提供する。

PPTPアクセスコンセントレータ (PAC)

外部コネクティビティ (典型的には1つかそれ以上のPSTN又はISDN回線を介して) を供給する装置。PPP動作及びPPTPプロトコルを取り扱うことができる。PACはIPを使用してユーザトラフィックを1つないし複数のPHSにトンネリングする。非IPプロトコルをトンネリングする場合もある。

PPTPネットワークサーバ (PNS)

汎用計算/サーバプラットフォーム上で動作するように設計された通信シャシ。PPTPプロトコルのサーバ側を取り扱う。PPTPが完全にIPに依存し、インタフェースハードウェアからは独立しているため、PNSはLAN、WAN装置を含むどのようなIPイン

タフェースハードウェアの組み合わせも使用することができる。

ポイントツーポイントトンネリングプロトコル (PPTP)

PACとPNS間のPPPトラフィックをトンネリングするために定義されたプロトコル。GRE (Generic Routing Encapsulation; 汎用ルーティングカプセル化) 機構を使用して、PPP packetsを伝送するためのフロー・輻輳制御カプセル化データグラムサービスを提供する。「トンネル」制御及び機能管理も支援し、制御接続の設定・解除、及びデータ接続の設定・解除を行う。PACとPNSのそれぞれの対に対して1つの制御接続と1つのデータ接続がある。

公衆交換電話回線網 (PSTN)

今日、3 KHz回線音声サーバを世界中の固定終点に供給する、陸上遠隔通信インフラストラクチャ。

リモート認証ダイヤルインユーザサービス (RADIUS)

ユーザ接続要求を受入れ、ユーザ認証を行い、クライアントがサービスをユーザに送るために必要な全ての構成情報を返送する。RADIUSサービスは他のRADIUSサーバ又は他の種類の認証サーバに対して

プロキシクライアントとしての役割を果たすことができる。RADIUSサーバはPPP PAP、CHAP、UNIXログイン、及びその他の認証機構を支援する。

TELNET

TelnetはTCP/IP接続を介しての2つのネットワーク仮想端末(NVT)間の非同期通信を支援するよう設計されている。NVTは、接続の両者すなわちクライアントとサーバがそれらの実際の出力及び入力端末をマップする仮想の装置である。

時分割多重アクセス(TDMA)

携帯電話及びPCSスペクトルでのデータワイヤレス遠隔通信のための北米基準。無線インタフェース上でユーザを多重化する技術。

伝送制御プロトコル(TCP)

IPネットワーク上におけるユーザデータの高信頼度コネクション型伝送機構。

TS-IP

トンネリングサーバIPアドレス

ユーザデータグラムプロトコル(UDP)

IP上に構築されたコネクションレス型プロトコル。サービスアクセス(SAP)はUDPポートとIPアドレスにより識別される。

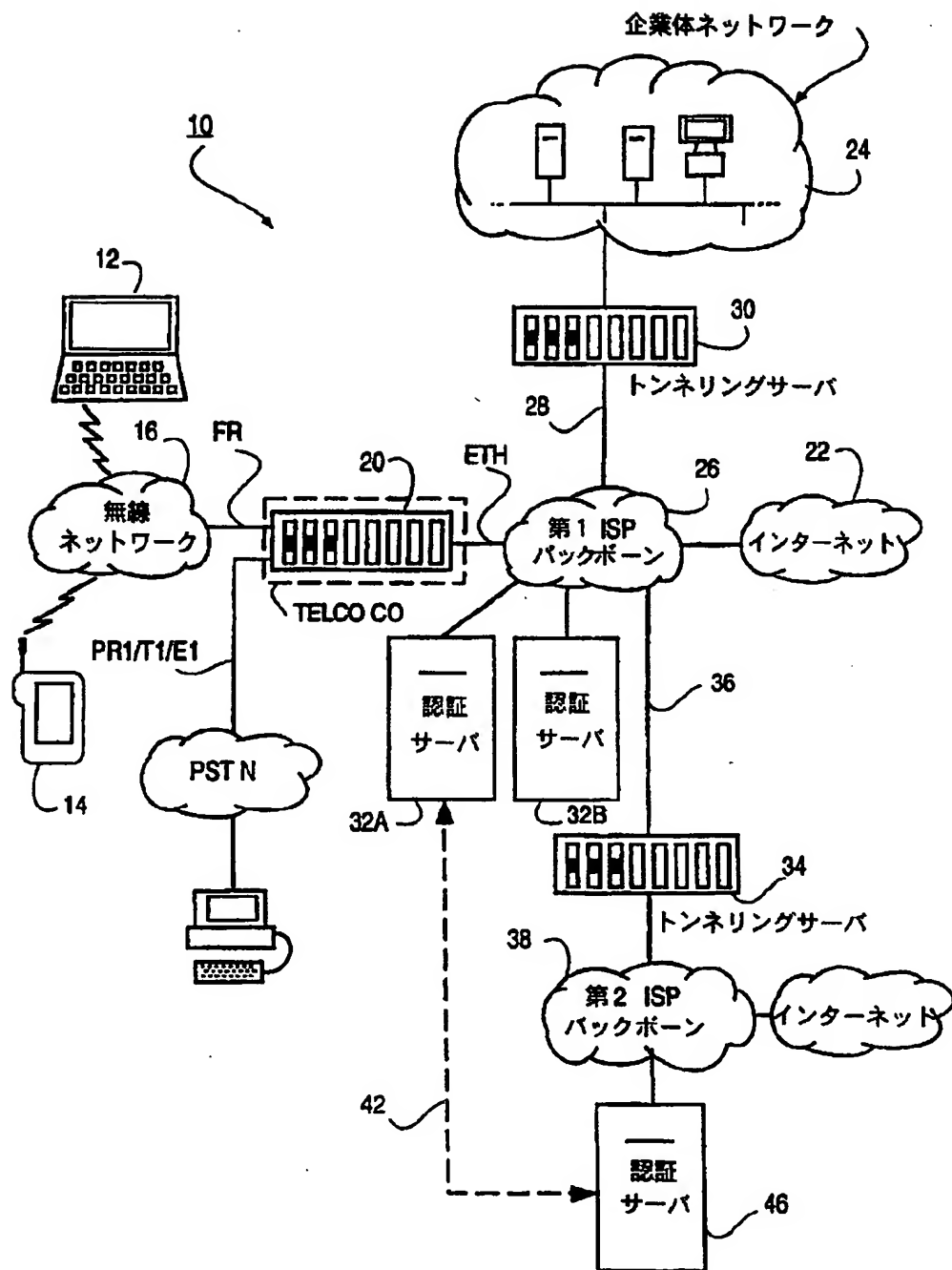
仮想プライベートネットワーク(VPN)

安全な情報アクセスを送るためのインターネット上に築かれた安全なネットワーク。

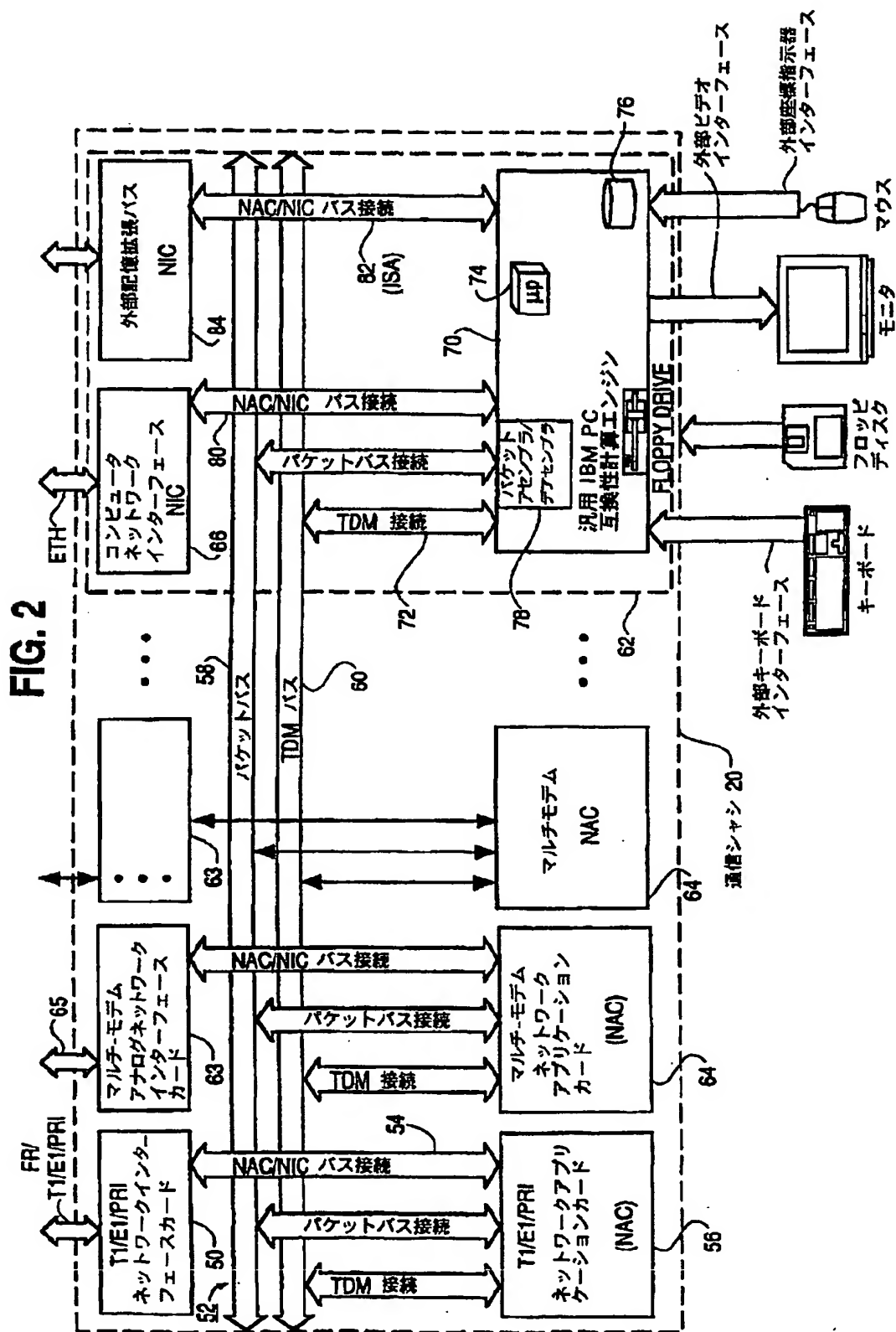
ここに開示した実施例に対しては、本発明の意図および範囲から逸脱することなく様々な変更ないし変形が可能であることが当業者には明らかである。この発明の精神並びに範囲は請求の範囲に記載の通りであり、該記載は上述の詳細な説明に照らして解釈されるものである。

【図1】

FIG. 1

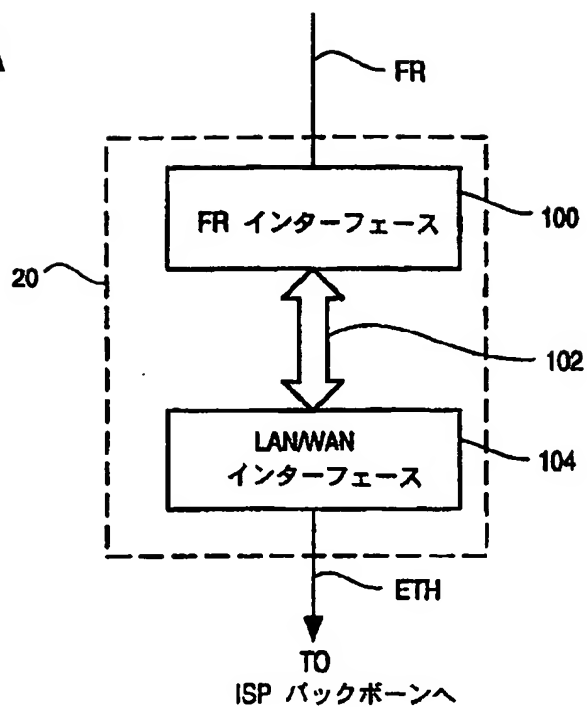


【図2】



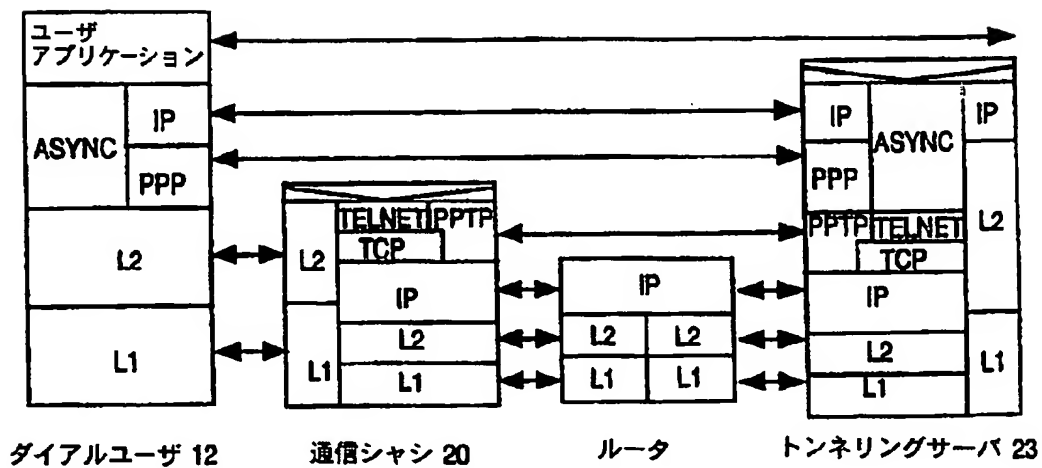
【図 2】

FIG. 2A



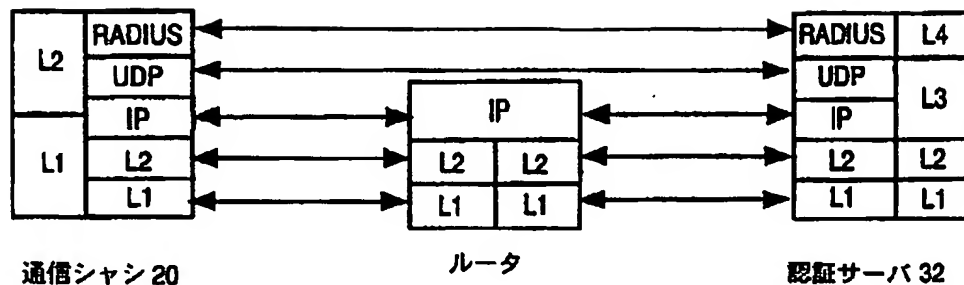
【図 3】

FIG. 3



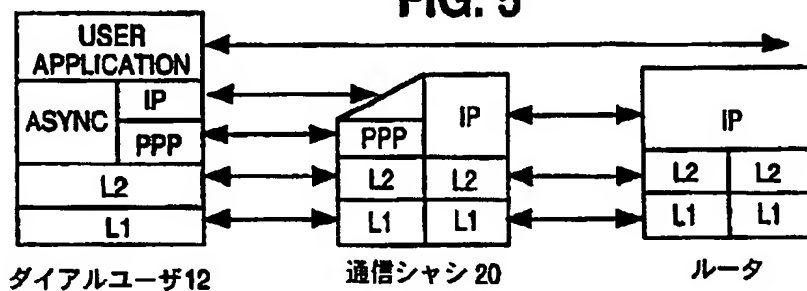
【図 4】

FIG. 4

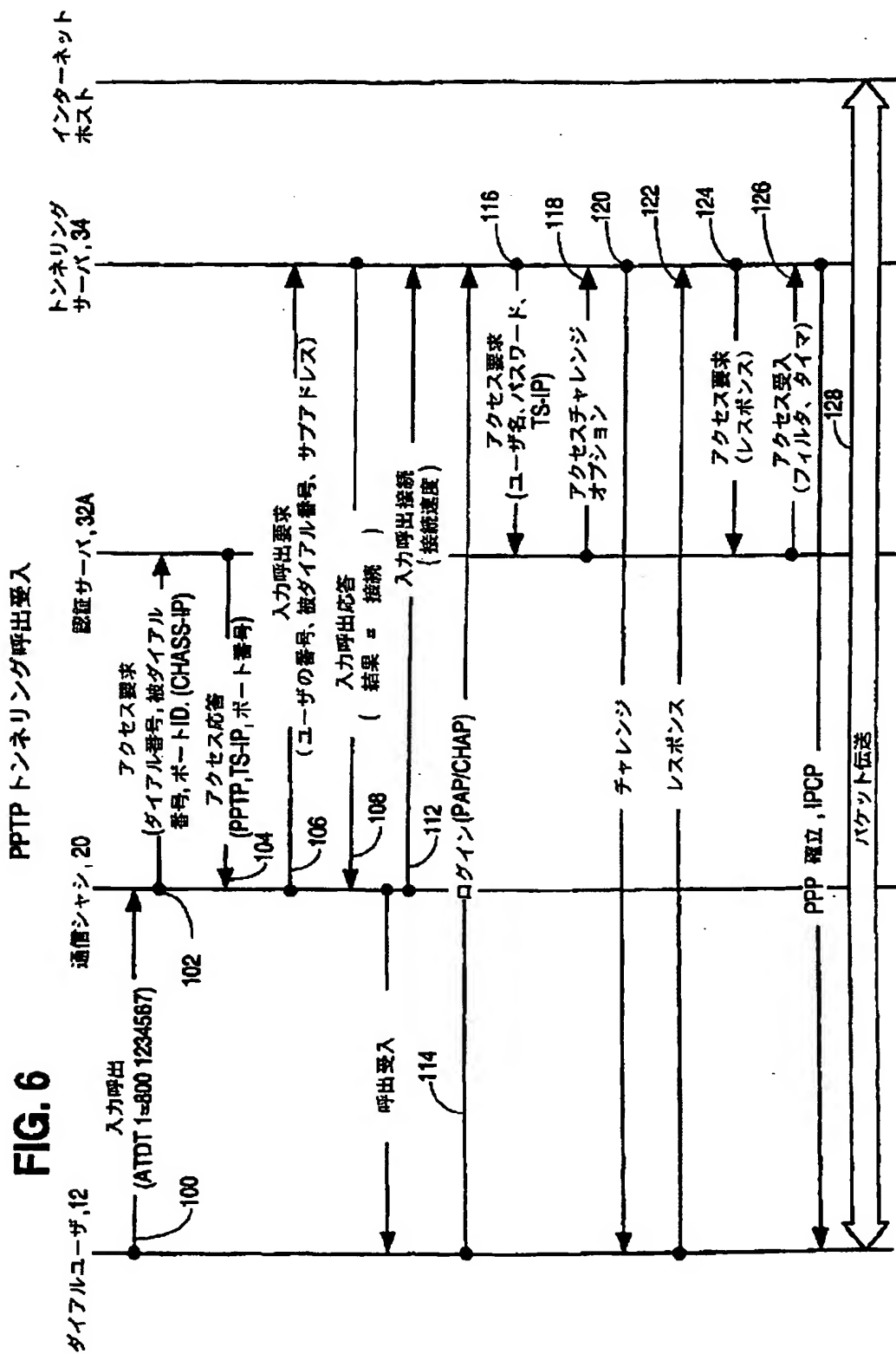


【図 5】

FIG. 5

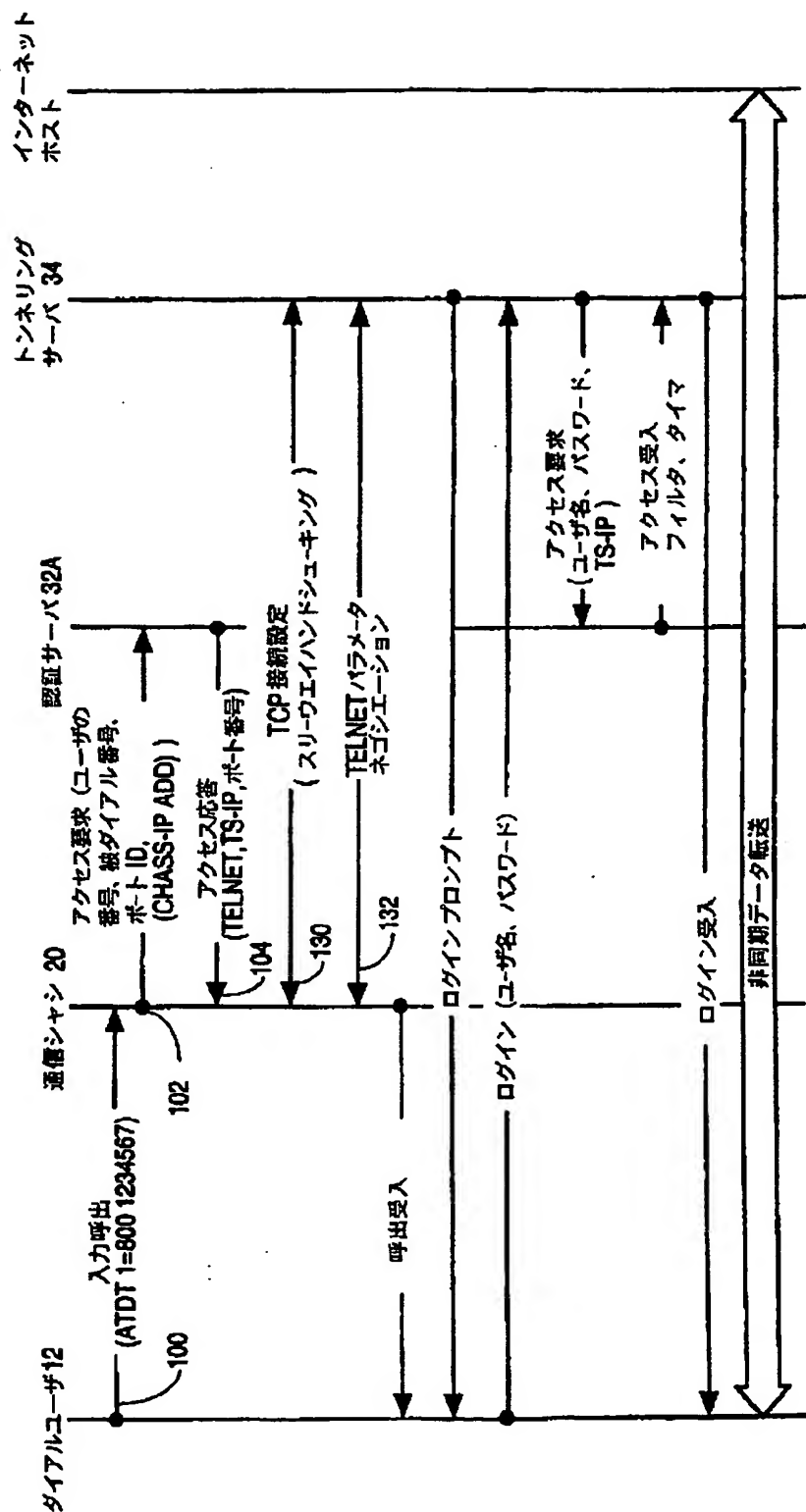


【図6】



【図 7】

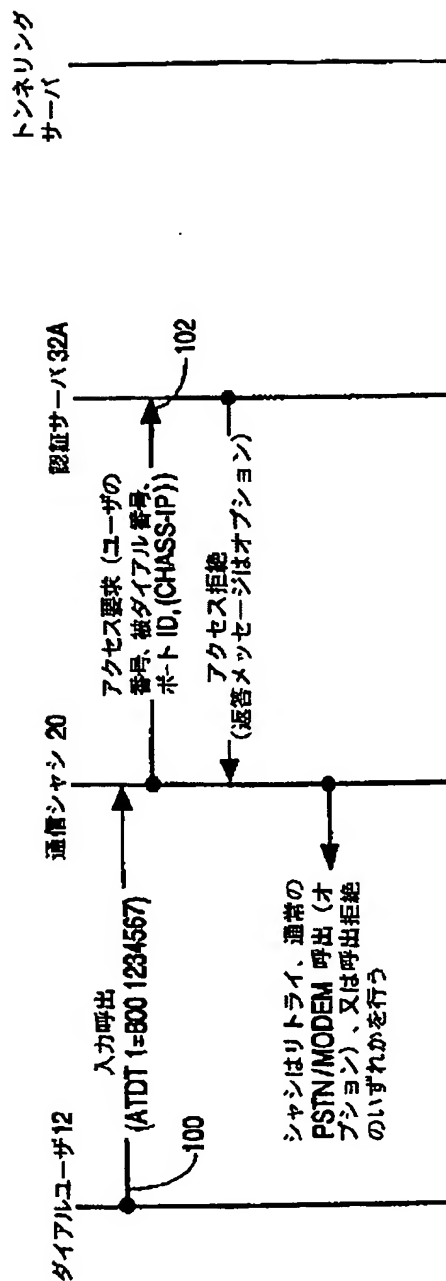
FIG. 7 TELNET トンネリング呼出受入



【図8】

FIG. 8

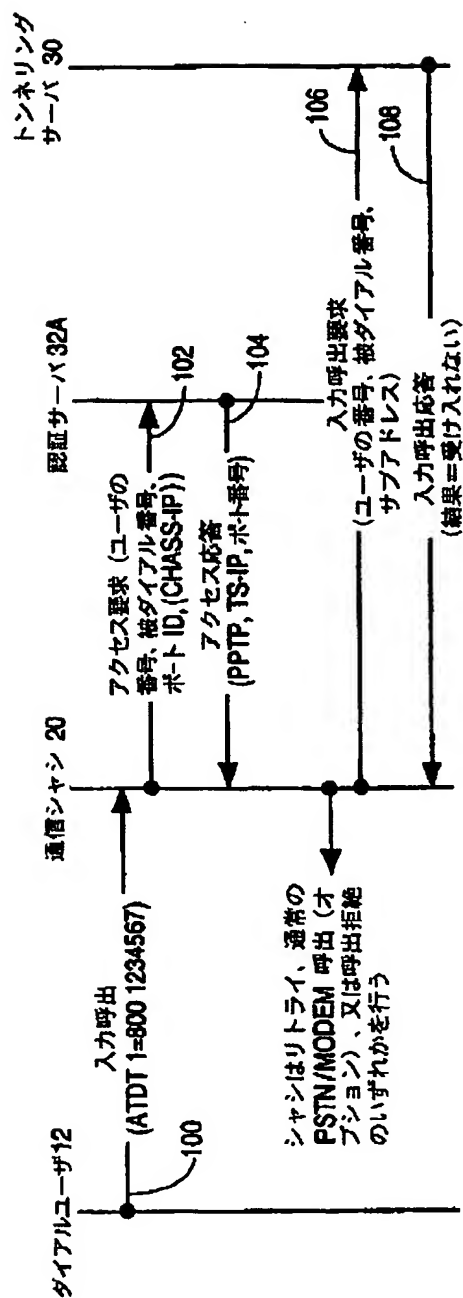
第1段階認証失敗



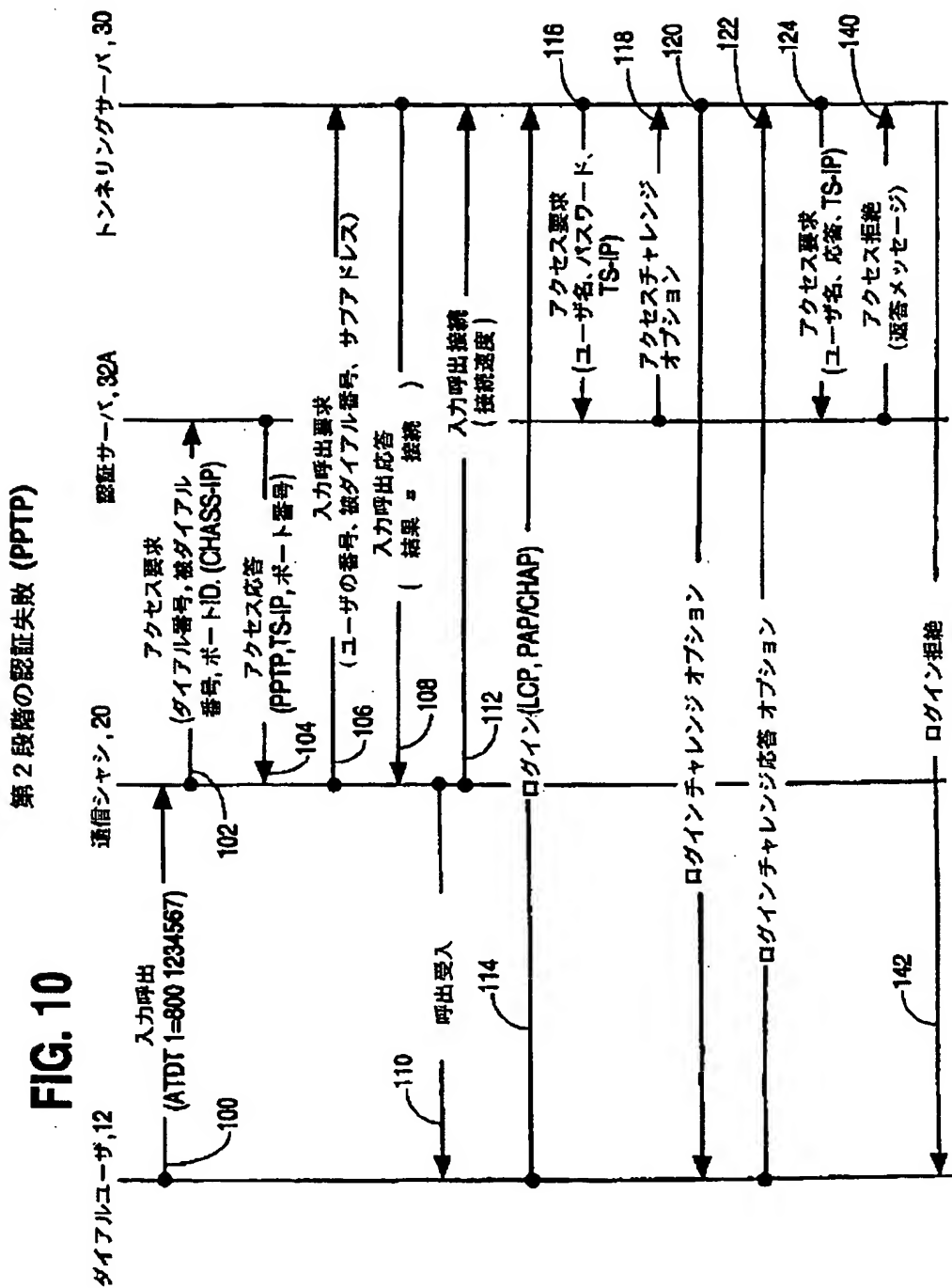
【図9】

トンネリングサーバアクセス拒絶 (PPTP)

FIG. 9



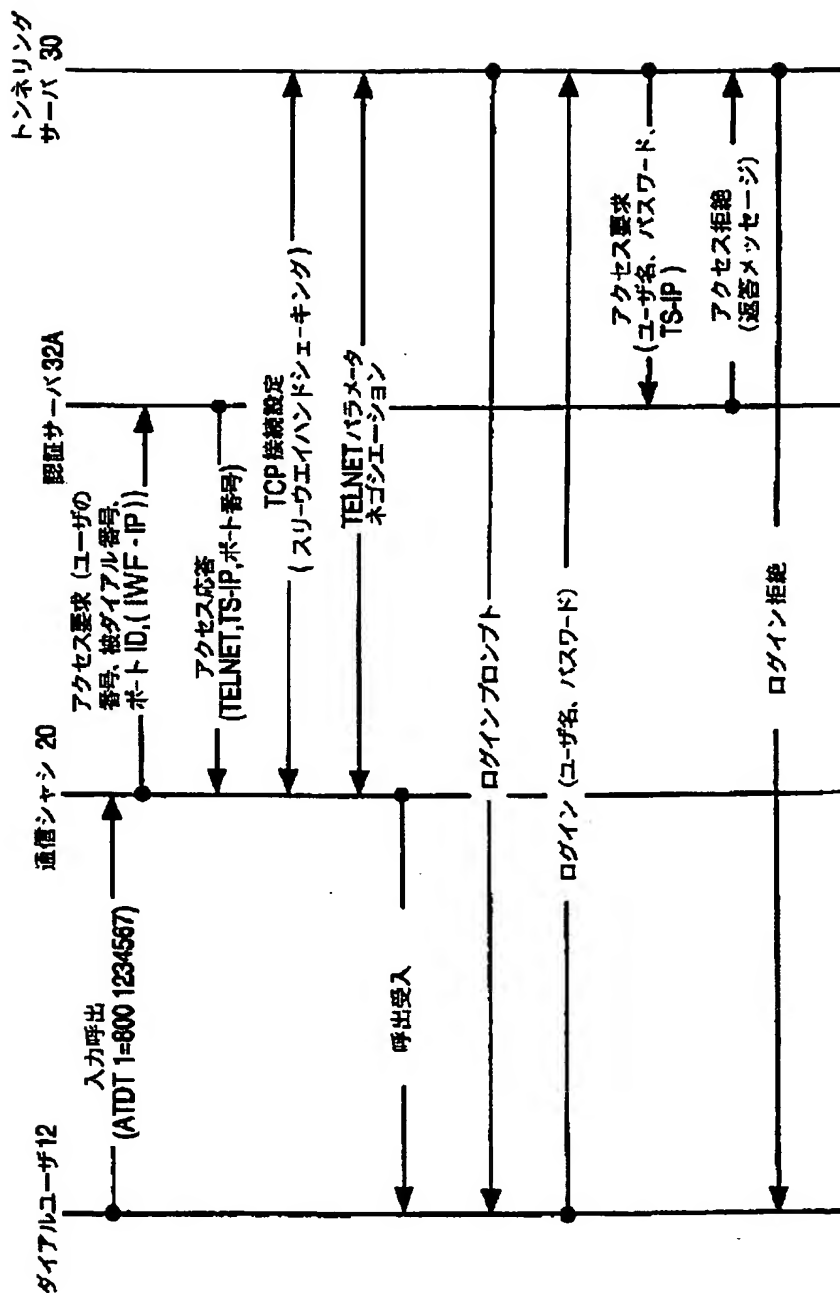
【図10】



【図11】

認証失敗 (TELNET)

FIG. 11



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US 98/13858

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>VARMA V K ET AL: "ARCHITECTURE FOR INTERWORKING DATA OVER PCS" IEEE COMMUNICATIONS MAGAZINE, vol. 34, no. 9, September 1996, pages 124-130, XP000627245 see abstract see page 126, left-hand column, line 12 - page 127, left-hand column, line 8 see page 128, left-hand column, line 23 - page 128, right-hand column, line 9 see page 129, left-hand column, line 52 - page 130, left-hand column, line 14 see figures 2,7,10</p> <p style="text-align: center;">-- -/--</p>	1-8, 17, 18

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"A" document member of the same patent family

Date of the actual completion of the international search

16 November 1998

Date of mailing of the international search report

23/11/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentplan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3018

Authorized officer

Lázaro López, M.L.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 98/13858

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 762 261 A (CADIX INC) 12 March 1997 see abstract see column 2, line 38 - column 4, line 20 see column 8, line 42-49 see column 9, line 6-9 see figures 1A,1B ---	9,11
A	WO 95 08900 A (NOKIA TELECOMMUNICATIONS OY ;WARSTA MARKUS (FI); JOKIAHO TIMO (FI)) 30 March 1995 see abstract see page 4, line 1-12 see page 4, line 24 - page 5, line 25 see page 5, line 34 - page 6, line 8 see page 6, line 14 - page 9, line 16 see page 9, line 25 - page 10, line 24. see figure 1 ---	1-8
A	KYLAENPAEAE M ET AL: "NOMADIC ACCESS TO INFORMATION SERVICES BY A GSM PHONE" COMPUTERS AND GRAPHICS, vol. 20, no. 5, 1 September 1996, pages 651-658, XP002037372 see abstract see page 652, left-hand column, line 16-30 see page 653, left-hand column, line 5-30 ---	1,17
A	PERKINS C ET AL: "IMHP: A mobile host protocol for the Internet" COMPUTER NETWORKS AND ISDN SYSTEMS, vol. 27, no. 3, December 1994, page 479-491 XP004037981 see abstract see page 483, right-hand column, line 1 - page 486, left-hand column, line 23 -----	2,3, 8-13,16

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. Application No

PCT/US 98/13858

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0762261 A	12-03-1997	JP 9081518 A	28-03-1997
		JP 9081519 A	28-03-1997
		JP 9081520 A	28-03-1997
		US 5706427 A	06-01-1998
WO 9508900 A	30-03-1995	FI 934115 A	21-03-1995
		AU 678534 B	29-05-1997
		AU 7658694 A	10-04-1995
		CN 1133666 A	16-10-1996
		EP 0720806 A	10-07-1996
		JP 9505951 T	10-06-1997

フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
H04M 3/00		H04L 11/00	310C
11/00	303	H04B 7/26	109M
H04Q 7/38			109S

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), UA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW

【要約の続き】

トワークへのアクセスを許可する、という各ステップを有する。

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.